Compliance and Regulatory Framework Industries

NIST Framework cyber security framework

<https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework>

The **NIST Cybersecurity Framework** provides a policy framework of [computer security](https://en.wikipedia.org/wiki/Computer_security) guidance for how [private sector](https://en.wikipedia.org/wiki/Private_sector) organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks. The framework has been translated to many languages and is used by the governments of Japan and Israel, among others.[[1]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-1) It "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes." Version 1.0 was published by the US [National Institute of Standards and Technology](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) in 2014, originally aimed at operators of [critical infrastructure](https://en.wikipedia.org/wiki/Critical_infrastructure). It is being used by a wide range of businesses and organizations and helps shift organizations to be proactive about risk management.[[2]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-2)[[3]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-3)[[4]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-4) In 2017, a draft version of the framework, version 1.1, was circulated for public comment.[[5]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-5) Version 1.1 was announced and made publicly available on April 16, 2018.[[6]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-6) Version 1.1 is still compatible with version 1.0. The changes include guidance on how to perform self-assessments, additional detail on supply chain risk management, guidance on how to interact with supply chain stakeholders, and encourages a [vulnerability disclosure](https://en.wikipedia.org/wiki/Vulnerability_disclosure) process.[[7]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-7)[[8]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-8)

A security framework adoption study reported that 70% of the surveyed organizations see NIST's framework as a popular best practice for computer security, but many note that it requires significant investment.[[9]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-9)

It includes guidance on relevant protections for [privacy](https://en.wikipedia.org/wiki/Privacy) and [civil liberties](https://en.wikipedia.org/wiki/Civil_liberties).[[10]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-10)

In 2017, NIST published the NIST Baldrige Cyber Security Excellence Builder which leverages the 2014 framework. It includes a simpler self-assessment.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] The questions are divided into six areas and a results section:[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

* Leadership
* Strategy
* Customers
* Measurement, Analysis and Knowledge Management
* Workforce
* Operations, and
* Results.



**Contents**

* [1Overview](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#Overview)
* [2Functions and categories of cybersecurity activities](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#Functions_and_categories_of_cybersecurity_activities)
  + [2.1Identify](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#Identify)
  + [2.2Protect](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#Protect)
  + [2.3Detect](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#Detect)
  + [2.4Respond](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#Respond)
  + [2.5Recover](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#Recover)
* [3See also](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#See_also)
* [4References](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#References)
* [5External links](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#External_links)

Overview[[edit](https://en.wikipedia.org/w/index.php?title=NIST_Cybersecurity_Framework&action=edit&section=1)]

The NIST Cybersecurity Framework is designed for individual businesses and other organizations to use to assess risks they face.

The framework is divided into three parts, "Core", "Profile" and "Tiers". The "Framework Core" contains an array of activities, outcomes and references about aspects and approaches to cybersecurity. The "Framework Implementation Tiers" are used by an organization to clarify for itself and its partners how it views cybersecurity risk and the degree of sophistication of its management approach. A "Framework Profile" is a list of outcomes that an organization has chosen from the categories and subcategories, based on its needs and risk assessments.

An organization typically starts by using the framework to develop a "Current Profile" which describes its cybersecurity activities and what outcomes it is achieving. It can then develop a "Target Profile", or adopt a baseline profile tailored to its sector (e.g. infrastructure industry) or type of organization. It can then define steps switch from its current profile to its target profile.

Functions and categories of cybersecurity activities[[edit](https://en.wikipedia.org/w/index.php?title=NIST_Cybersecurity_Framework&action=edit&section=2)]

The NIST Cybersecurity Framework organizes its "core" material into five "functions" which are subdivided into a total of 23 "categories". For each category, it defines a number of subcategories of cybersecurity outcomes and [security controls](https://en.wikipedia.org/wiki/Security_control), with 108 subcategories in all.

For each subcategory, it also provides "Informative Resources" referencing specific sections of a variety of other information security standards, including [ISO 27001](https://en.wikipedia.org/wiki/ISO/IEC_27001:2013), [COBIT](https://en.wikipedia.org/wiki/COBIT), NIST SP 800-53, ANSI/ISA-62443, and the [Council on CyberSecurity Critical Security Controls](https://en.wikipedia.org/wiki/The_Center_for_Internet_Security_Critical_Security_Controls_for_Effective_Cyber_Defense) (CCS CSC, now managed by the [Center for Internet Security](https://en.wikipedia.org/wiki/Center_for_Internet_Security)). Special Publications (SP) aside, most of the informative references requires a paid membership or purchase to access their respective guides. The cost and complexity of the framework has resulted in bills from both houses of Congress that direct NIST to create Cybersecurity Framework guides that are more accessible to small and medium businesses.[[11]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-11)[[12]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-12)

Here are the functions and categories, along with their unique identifiers and definitions, as stated in the category column of its spreadsheet view of the core of the standard.[[13]](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework#cite_note-13)

**Identify**[[edit](https://en.wikipedia.org/w/index.php?title=NIST_Cybersecurity_Framework&action=edit&section=3)]

"Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities."

* Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
* Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
* Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
* Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
* Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
* Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.

**Protect**[[edit](https://en.wikipedia.org/w/index.php?title=NIST_Cybersecurity_Framework&action=edit&section=4)]

"Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services."

* Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
* Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
* Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
* Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
* Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
* Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

**Detect**[[edit](https://en.wikipedia.org/w/index.php?title=NIST_Cybersecurity_Framework&action=edit&section=5)]

"Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event."

* Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.
* Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
* Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

**Respond**[[edit](https://en.wikipedia.org/w/index.php?title=NIST_Cybersecurity_Framework&action=edit&section=6)]

"Develop and implement the appropriate activities to take action regarding a detected cybersecurity event."

* Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
* Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
* Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
* Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
* Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

**Recover**[[edit](https://en.wikipedia.org/w/index.php?title=NIST_Cybersecurity_Framework&action=edit&section=7)]

"Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event."

* Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
* Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
* Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

See also[[edit](https://en.wikipedia.org/w/index.php?title=NIST_Cybersecurity_Framework&action=edit&section=8)]

* [Cyber security standards](https://en.wikipedia.org/wiki/Cyber_security_standards)
* [Critical infrastructure protection](https://en.wikipedia.org/wiki/Critical_infrastructure_protection)
* [ISO/IEC 27001:2013](https://en.wikipedia.org/wiki/ISO/IEC_27001:2013): an information security standard from the [International Organization for Standardization](https://en.wikipedia.org/wiki/International_Organization_for_Standardization)
* [COBIT](https://en.wikipedia.org/wiki/COBIT): Control Objectives for Information and Related Technologies - a related framework from [ISACA](https://en.wikipedia.org/wiki/ISACA)
* [NIST Special Publication 800-53](https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53): “Security and Privacy Controls for Federal Information Systems and Organizations."
* [Cyber Risk Quantification](https://en.wikipedia.org/wiki/Cyber_Risk_Quantification)

CMMC Cybersecurity Maturity Model Certification

<https://www.acq.osd.mil/cmmc/index.html>

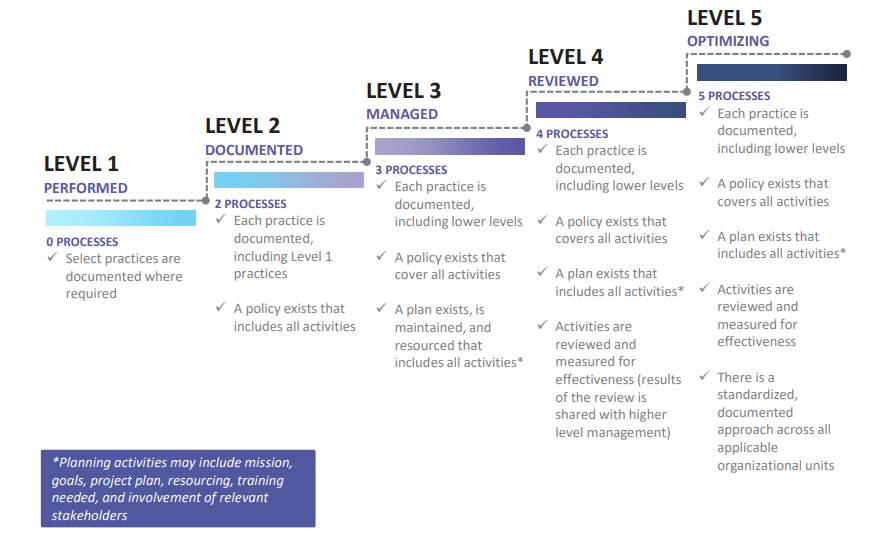
The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) recognizes that security is foundational to acquisition and should not be traded along with cost, schedule, and performance moving forward. The Department is committed to working with the Defense Industrial Base (DIB) sector to enhance the protection of controlled unclassified information (CUI) within the supply chain.

OUSD(A&S) is working with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry to develop the Cybersecurity Maturity Model Certification (CMMC).

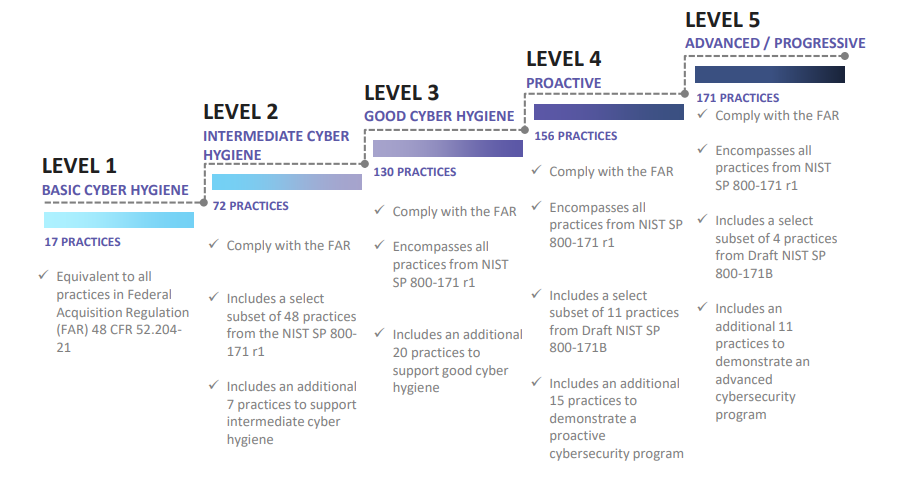
* The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.
* The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.
* The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.
* The intent is for certified independent 3rd party organizations to conduct audits and inform risk.

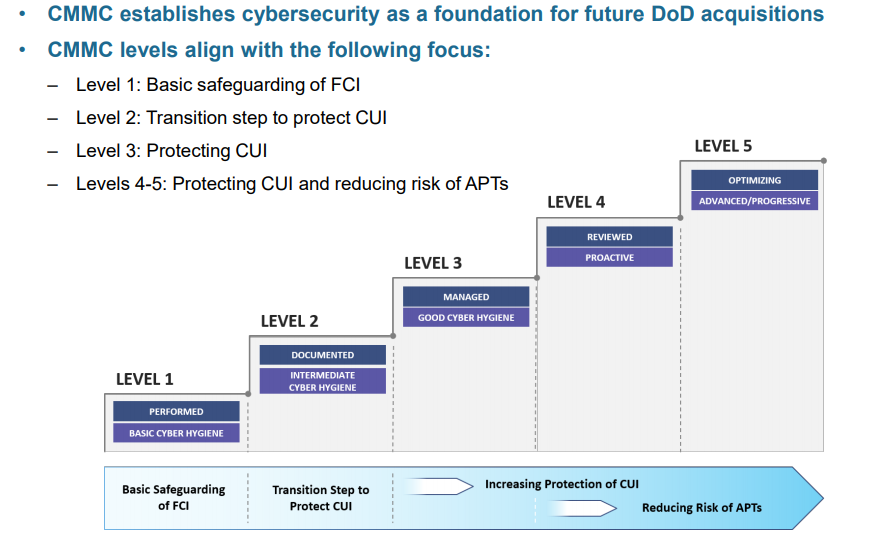
<https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf>

CMMC Practice Progression



CMMC Practice Progression





About PCI DSS Industries Retail, Healthcare, Financial

Payment Card Industry Data Security Standard

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#p-search)

|  |  |
| --- | --- |
|  | This article **needs additional citations for**[**verification**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability). Please help [improve this article](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit) by [adding citations to reliable sources](https://en.wikipedia.org/wiki/Help:Introduction_to_referencing_with_Wiki_Markup/1). Unsourced material may be challenged and removed. *Find sources:* ["Payment Card Industry Data Security Standard"](https://www.google.com/search?as_eq=wikipedia&q=%22Payment+Card+Industry+Data+Security+Standard%22) – [news](https://www.google.com/search?tbm=nws&q=%22Payment+Card+Industry+Data+Security+Standard%22+-wikipedia) **·** [newspapers](https://www.google.com/search?&q=%22Payment+Card+Industry+Data+Security+Standard%22+site:news.google.com/newspapers&source=newspapers) **·** [books](https://www.google.com/search?tbs=bks:1&q=%22Payment+Card+Industry+Data+Security+Standard%22+-wikipedia) **·** [scholar](https://scholar.google.com/scholar?q=%22Payment+Card+Industry+Data+Security+Standard%22) **·** [JSTOR](https://www.jstor.org/action/doBasicSearch?Query=%22Payment+Card+Industry+Data+Security+Standard%22&acc=on&wc=on) *(October 2017) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

|  |  |
| --- | --- |
|  | This article contains references that [**appear to be spam**](https://en.wikipedia.org/wiki/Wikipedia:What_Wikipedia_is_not#Wikipedia_is_not_a_soapbox_or_means_of_promotion). Wikipedia is not a collection of links and should not be used for advertising. Please help [improve this article](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit) by [adding citations to reliable sources](https://en.wikipedia.org/wiki/Help:Introduction_to_referencing_with_Wiki_Markup/1). See [Wikipedia:External links](https://en.wikipedia.org/wiki/Wikipedia:External_links) and [Wikipedia:Spam](https://en.wikipedia.org/wiki/Wikipedia:Spam) for details. *(December 2018) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

The **Payment Card Industry Data Security Standard** (**PCI DSS**) is an [information security](https://en.wikipedia.org/wiki/Information_security) standard for organizations that handle branded [credit cards](https://en.wikipedia.org/wiki/Credit_card) from the major [card schemes](https://en.wikipedia.org/wiki/Card_scheme).

The PCI Standard is mandated by the card brands but administered by the [Payment Card Industry Security Standards Council](https://en.wikipedia.org/wiki/Payment_Card_Industry_Security_Standards_Council). The standard was created to increase controls around cardholder data to reduce [credit card fraud](https://en.wikipedia.org/wiki/Credit_card_fraud). Validation of compliance is performed annually or quarterly,[[1]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-1)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)] either by an external [Qualified Security Assessor](https://en.wikipedia.org/wiki/Qualified_Security_Assessor) (QSA) or by a firm specific [Internal Security Assessor (ISA)](https://en.wikipedia.org/wiki/Internal_Security_Assessor_(ISA)) that creates a Report on Compliance for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.[[2]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-Mehmood-IntroIntoPCIDSS-2)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)][[3]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-PCI_DSS-3)



**Contents**

* [1History](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#History)
* [2Requirements](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Requirements)
* [3Updates and supplemental information](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Updates_and_supplemental_information)
* [4Compliance levels](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Compliance_levels)
* [5Validation of compliance](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Validation_of_compliance)
  + [5.1Qualified Security Assessor (QSA)](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Qualified_Security_Assessor_(QSA))
  + [5.2Internal Security Assessor (ISA)](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Internal_Security_Assessor_(ISA))
  + [5.3Report on Compliance (ROC)](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Report_on_Compliance_(ROC))
  + [5.4Self-Assessment Questionnaire (SAQ)](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Self-Assessment_Questionnaire_(SAQ))
* [6Compliance versus validation of compliance](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Compliance_versus_validation_of_compliance)
* [7Legislation](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Legislation)
* [8Risk management to protect cardholder data](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Risk_management_to_protect_cardholder_data)
* [9Controversies and criticisms](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Controversies_and_criticisms)
  + [9.1Compliance and compromises](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Compliance_and_compromises)
* [10See also](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#See_also)
* [11References](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#References)
* [12Further reading](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#Further_reading)
* [13External links](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#External_links)

History[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=1)]

Five different programs have been started by card companies:

* [Visa](https://en.wikipedia.org/wiki/Visa_(company))'s [Cardholder Information Security Program](https://en.wikipedia.org/wiki/Cardholder_Information_Security_Program)
* [MasterCard](https://en.wikipedia.org/wiki/MasterCard)'s Site Data Protection
* [American Express](https://en.wikipedia.org/wiki/American_Express)'s Data Security Operating Policy
* [Discover](https://en.wikipedia.org/wiki/Discover_Card)'s Information Security and Compliance
* the [JCB](https://en.wikipedia.org/wiki/Japan_Credit_Bureau)'s Data Security Program

The intentions of each were roughly similar: to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process, and transmit cardholder data. To cater out the interoperability problems among the existing standards, the combined effort made by the principal credit card organizations resulted in the release of version 1.0 of PCI DSS in December 2004. PCI DSS has been implemented and followed across the globe.[[2]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-Mehmood-IntroIntoPCIDSS-2)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)]

The Payment Card Industry Security Standards Council (PCI SSC) was then formed and these companies aligned their individual policies to create the PCI DSS.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] MasterCard, American Express, Visa, JCB International and Discover Financial Services established the PCI SSC in September 2006 as an administration/governing entity which mandates the evolution and development of PCI DSS. Independent/private organizations can participate in PCI development after proper registration. Each participating organization joins a particular SIG (Special Interest Group) and contributes to the activities which are mandated by the SIG.[[2]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-Mehmood-IntroIntoPCIDSS-2)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)]

The following versions of the PCI DSS have been made available:[[2]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-Mehmood-IntroIntoPCIDSS-2)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)]

* 1.0 was released on December 15, 2004.
* 1.1 in September 2006 provide clarification and minor revisions.
* 1.2 was released on October 1, 2008. It enhanced clarity, improved flexibility, and addressed evolving risks and threats.
* 1.2.1 in August 2009 made minor corrections designed to create more clarity and consistency among the standards and supporting documents.
* 2.0 was released in October 2010.
* 3.0 was released in November 2013 and was active from January 1, 2014 to June 31, 2015.
* 3.1 was released in April 2015, and has been retired since October 31, 2016.
* 3.2 was released in April 2016, and has been retired since December 31, 2018.
* 3.2.1 was released in May 2018.

Requirements[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=2)]

The PCI Data Security Standard specifies twelve requirements for compliance, organized into six logically related groups called "control objectives". The six groups are:[[2]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-Mehmood-IntroIntoPCIDSS-2)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)]

1. Build and Maintain a Secure Network and Systems
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

Each version of PCI DSS (Payment Card Industry Data Security Standard) has divided these six requirements into a number of sub-requirements differently, but the twelve high-level requirements have not changed since the inception of the standard. Each requirement/sub-requirement is additionally elaborated into three sections.[[2]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-Mehmood-IntroIntoPCIDSS-2)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)]

1. Requirement Declaration: It defines the main description of the requirement. The endorsement of PCI DSS is done on the proper implementation of the requirements.
2. Testing Processes: The processes and methodologies carried out by the assessor for the confirmation of proper implementation.
3. Guidance: It explains the core purpose of the requirement and the corresponding content which can assist in the proper definition of the requirement.

The twelve requirements for building and maintaining a secure network and systems can be summarized as follows:[[4]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-Turner-12-requirements-4)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)]

1. Installing and maintaining a firewall configuration to protect cardholder data. The purpose of a firewall is to scan all network traffic, block untrusted networks from accessing the system.
2. Changing vendor-supplied defaults for system passwords and other security parameters. These passwords are easily discovered through public information and can be used by malicious individuals to gain unauthorized access to systems.
3. Protecting stored cardholder data. Encryption, hashing, masking and truncation are methods used to protect card holder data.
4. Encrypting transmission of cardholder data over open, public networks. Strong encryption, including using only trusted keys and certifications reduces risk of being targeted by malicious individuals through hacking.
5. Protecting all systems against malware and performing regular updates of anti-virus software. Malware can enter a network through numerous ways, including Internet use, employee email, mobile devices or storage devices. Up-to-date anti-virus software or supplemental anti-malware software will reduce the risk of exploitation via malware.
6. Developing and maintaining secure systems and applications. Vulnerabilities in systems and applications allow unscrupulous individuals to gain privileged access. Security patches should be immediately installed to fix vulnerability and prevent exploitation and compromise of cardholder data.
7. Restricting access to cardholder data to only authorized personnel. Systems and processes must be used to restrict access to cardholder data on a “need to know” basis.
8. Identifying and authenticating access to system components. Each person with access to system components should be assigned a unique identification (ID) that allows accountability of access to critical data systems.
9. Restricting physical access to cardholder data. Physical access to cardholder data or systems that hold this data must be secure to prevent the unauthorized access or removal of data.
10. Tracking and monitoring all access to cardholder data and network resources. Logging mechanisms should be in place to track user activities that are critical to prevent, detect or minimize impact of data compromises.
11. Testing security systems and processes regularly. New vulnerabilities are continuously discovered. Systems, processes and software need to be tested frequently to uncover vulnerabilities that could be used by malicious individuals.
12. Maintaining an information security policy for all personnel. A strong security policy includes making personnel understand the sensitivity of data and their responsibility to protect it.

Updates and supplemental information[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=3)]

The PCI SSC(Payment Card Industry Security Standards Council) has released several supplemental pieces of information to clarify various requirements. These documents include the following [[2]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-Mehmood-IntroIntoPCIDSS-2)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)]

* Information Supplement: Requirement 11.3 Penetration Testing
* Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified
* Navigating the PCI DSS - Understanding the Intent of the Requirements
* [*"Information Supplement: PCI DSS Wireless Guidelines"*](https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Wireless_Guidelines.pdf)*(PDF). August 26, 2011.*
* PCI DSS Applicability in an EMV Environment [[5]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-MEHMOOD-PKI-EMV-5)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)]
* Prioritized Approach for PCI DSS
* Prioritized Approach Tool
* PCI DSS Quick Reference Guide
* PCI DSS Virtualization Guidelines
* PCI DSS Tokenization Guidelines
* PCI DSS 2.0 Risk Assessment Guidelines
* The lifecycle for Changes to the PCI DSS and PA-DSS
* Guidance for PCI DSS Scoping and Segmentation

Compliance levels[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=4)]

All companies who are subject to PCI DSS standards must be PCI compliant. There are four levels of PCI Compliance and these are based on how much you process per year, as well as other details about the level of risk assessed by payment brands.[[6]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-6)

At a high level, the levels are following:

* Level 1 – Over 6 million transactions annually
* Level 2 – Between 1 and 6 million transactions annually
* Level 3 – Between 20,000 and 1 million transactions annually
* Level 4 – Less than 20,000 transactions annually

Each card issuer maintains their own table of compliance levels.[[7]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-7)[[8]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-8)

Validation of compliance[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=5)]

Compliance validation involves the evaluation and confirmation that the security controls & procedures have been properly implemented as per the policies recommended by PCI DSS. In short, the PCI DSS, security validation/testing procedures mutually as compliance validation tool. A PCI DSS assessment has the following entities. [[9]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-MEHMOOD-compliance-9)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)][[10]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-PCI_Validation-10)

**Qualified Security Assessor (QSA)**[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=6)]

*Main article:*[*Qualified Security Assessor*](https://en.wikipedia.org/wiki/Qualified_Security_Assessor)

A Qualified Security Assessor is an individual bearing a certificate that has been provided by the PCI Security Standards Council. This certified person can audit merchants for Payment Card Industry Data Security Standard (PCI DSS) compliance. QSAs are the independent groups/entities which have been certified by PCI SSC for compliance confirmation in organization procedures. The confirmation just assigns that a QSA has tended to all the separate prerequisites which are mandatory to do PCI DSS appraisals. [[9]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-MEHMOOD-compliance-9)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)][[10]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-PCI_Validation-10)

**Internal Security Assessor (ISA)**[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=7)]

*Main article:*[*Internal Security Assessor (ISA)*](https://en.wikipedia.org/wiki/Internal_Security_Assessor_(ISA))

An Internal Security Assessor is an individual who has earned a certificate from the PCI Security Standards Company for their sponsoring organization. This certified person has the ability to perform PCI self-assessments for their organization. This ISA program was designed to help Level 2 merchants meet the new Mastercard compliance validation requirements.[[11]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-FierceRetail_2010-11) ISA certification empowers a worker to do an inward appraisal of his/her association and propose security solutions/ controls for the PCI DSS compliance. As the ISAs are upheld by the organization for the PCI SSC affirmation, they are in charge of cooperation and participation with QSAs.[[9]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-MEHMOOD-compliance-9)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)][[10]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-PCI_Validation-10)

**Report on Compliance (ROC)**[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=8)]

A Report on Compliance is a form that has to be filled by all level 1 merchants Visa merchants undergoing a PCI DSS (Payment Card Industry Data Security Standard) audit. The ROC form is used to verify that the merchant being audited is compliant with the PCI DSS standard. ROC confirms that policies, strategies, approaches & workflows are appropriately implemented/developed by the organization for the protection of cardholders against scams/frauds card-based business transactions. A template “ROC Reporting Template” available on PCI SSC site contains detailed guidelines about the ROC. [[9]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-MEHMOOD-compliance-9)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)][[10]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-PCI_Validation-10)

**Self-Assessment Questionnaire (SAQ)**[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=9)]

The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers report the results of their PCI DSS self-assessment.

The Self-Assessment Questionnaire is a set of Questionnaires documents that merchants are required to complete every year and submit to their transaction Bank. Another component of SAQ is Attestation of Compliance (AOC) where each SAQ question is replied based on the internal PCI DSS self-evaluation. Each SAQ question must be replied with yes or no alternative. In the event that a question has the appropriate response "no", at that point the association must highlight its future implementation aspects.[[9]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-MEHMOOD-compliance-9)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)][[10]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-PCI_Validation-10)

Compliance versus validation of compliance[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=10)]

Although the PCI DSS must be implemented by all entities that process, store or transmit cardholder data, formal validation of PCI DSS compliance is not mandatory for all entities. Currently both [Visa](https://en.wikipedia.org/wiki/Visa_Inc.) and [MasterCard](https://en.wikipedia.org/wiki/MasterCard) require merchants and service providers to be validated according to the PCI DSS. Visa also offers an alternative program called the Technology Innovation Program (TIP) that allows qualified merchants to discontinue the annual PCI DSS validation assessment. These merchants are eligible if they are taking alternative precautions against counterfeit fraud such as the use of [EMV](https://en.wikipedia.org/wiki/EMV) or [Point to Point Encryption](https://en.wikipedia.org/wiki/Point_to_Point_Encryption).

Issuing banks are not required to go through PCI DSS validation although they still have to secure the sensitive data in a PCI DSS compliant manner. Acquiring banks are required to comply with PCI DSS as well as to have their compliance validated by means of an audit.

In the event of a security breach, any compromised entity which was not PCI DSS compliant at the time of breach will be subject to additional card scheme penalties, such as fines.

Legislation[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=11)]

Compliance with PCI DSS is not required by federal law in the [United States](https://en.wikipedia.org/wiki/United_States). However, the laws of some U.S. states either refer to PCI DSS directly, or make equivalent provisions. The legal scholars Edward Morse and Vasant Raval have argued that, by enshrining PCI DSS compliance in legislation, the card networks have reallocated the externalized cost of fraud from the card issuers to merchants.[[12]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-morse-12)

In 2007, Minnesota enacted a law prohibiting the retention of some types of payment card data subsequent to 48 hours after authorization of the transaction.[[13]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-13)[[14]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-14)

In 2009, Nevada incorporated the standard into state law, requiring compliance of merchants doing business in that state with the current PCI DSS, and shields compliant entities from liability. The Nevada law also allows merchants to avoid liability by other approved security standards.[[15]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-15)[[12]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-morse-12)

In 2010, Washington also incorporated the standard into state law. Unlike Nevada's law, entities are not required to be compliant to PCI DSS, but compliant entities are shielded from liability in the event of a data breach.[[16]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-16)[[12]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-morse-12)

Risk management to protect cardholder data[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=12)]

Under PCI DSS’s requirement 3, merchants and financial institutions are implored to protect their clients’ sensitive data with strong cryptography. Non compliant solutions will not pass the audit.[[3]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-PCI_DSS-3) A typical [risk management](https://en.wikipedia.org/wiki/Risk_management) program can be structured in 3 steps:[[17]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-Crypto-Risks-17)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)]

1. Identify all known risks and record/describe them in a risk register. For example, [hardware security modules](https://en.wikipedia.org/wiki/Hardware_security_module) (HSM) that are used in the cryptographic [key management](https://en.wikipedia.org/wiki/Key_management) process could potentially introduce their own risks if compromised, whether physically or logically. HSMs create a root of trust within in the system. However, while it is unlikely, if the HSM is compromised, this could compromise the entire system.
2. Develop a risk management program is to analyze all identified risks. Included in this analysis should be a mix of qualitative and quantitative techniques to determine what risk [treatment methods](https://en.wikipedia.org/wiki/IT_risk_management) should be used to reduce the possibility of risks. For example, an organization might analyze the risk of using a cloud HSM versus a physical device that they use onsite.
3. Treat the risks in response to the risk analysis that was previously performed. For example, employing different treatments to protect client information stored in a cloud HSM versus ensuring security both physically and logically for an onsite HSM, which could include implementing controls or obtaining insurance to maintain an acceptable level of risk.

Continuous monitoring and review are part of the process of reducing PCI DSS cryptography risks. This includes maintenance schedules and predefined escalation and recovery routines when security weaknesses are discovered.[[17]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-Crypto-Risks-17)

Controversies and criticisms[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=13)]

|  |  |
| --- | --- |
|  | This section **needs additional citations for**[**verification**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability). Please help [improve this article](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit) by [adding citations to reliable sources](https://en.wikipedia.org/wiki/Help:Introduction_to_referencing_with_Wiki_Markup/1). Unsourced material may be challenged and removed. *Find sources:* ["Payment Card Industry Data Security Standard"](https://www.google.com/search?as_eq=wikipedia&q=%22Payment+Card+Industry+Data+Security+Standard%22) – [news](https://www.google.com/search?tbm=nws&q=%22Payment+Card+Industry+Data+Security+Standard%22+-wikipedia) **·** [newspapers](https://www.google.com/search?&q=%22Payment+Card+Industry+Data+Security+Standard%22+site:news.google.com/newspapers&source=newspapers) **·** [books](https://www.google.com/search?tbs=bks:1&q=%22Payment+Card+Industry+Data+Security+Standard%22+-wikipedia) **·** [scholar](https://scholar.google.com/scholar?q=%22Payment+Card+Industry+Data+Security+Standard%22) **·** [JSTOR](https://www.jstor.org/action/doBasicSearch?Query=%22Payment+Card+Industry+Data+Security+Standard%22&acc=on&wc=on) *(August 2018) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

Visa and Mastercard impose fines for non-compliance.[[18]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-18)[[*promotional source?*](https://en.wikipedia.org/wiki/Wikipedia:RS#Questionable_sources)]

Stephen and Theodora "Cissy" McComb, owners of Cisero’s Ristorante and Nightclub in Park City, Utah, were allegedly fined for a breach for which two forensics firms could not find evidence as having occurred:

"The PCI system is less a system for securing customer card data than a system for raking in profits for the card companies via fines and penalties. Visa and MasterCard impose fines on merchants even when there is no fraud loss at all, simply because the fines 'are profitable to them'."[[19]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-19)

Michael Jones, CIO of Michaels' Stores, testified before a U.S. Congress subcommittee regarding the PCI DSS:

"(...the PCI DSS requirements...) are very expensive to implement, confusing to comply with, and ultimately subjective, both in their interpretation and in their enforcement. It is often stated that there are only twelve 'Requirements' for PCI compliance. In fact there are over 220 sub-requirements; some of which can place an *incredible burden on a retailer* and *many of which are subject to interpretation*."[[20]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-20)

Others have suggested that PCI DSS is a step toward making all businesses pay more attention to IT security, even if minimum standards are not enough to completely eradicate security problems. For example, [Bruce Schneier](https://en.wikipedia.org/wiki/Bruce_Schneier) has spoken in favor of PCI DSS:

"Regulation—SOX, HIPAA, GLBA, the credit-card industry's PCI, the various disclosure laws, the European Data Protection Act, whatever—has been the best stick the industry has found to beat companies over the head with. And it works. Regulation forces companies to take security more seriously, and sells more products and services."[[21]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-21)

PCI Council General Manager Bob Russo's responded to the objections of the [National Retail Federation](https://en.wikipedia.org/wiki/National_Retail_Federation):

"[PCI is a structured] blend...[of] specificity and high-level concepts [that allows] stakeholders the opportunity and flexibility to work with Qualified Security Assessors (QSAs) to determine appropriate security controls within their environment that meet the intent of the PCI standards."[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**Compliance and compromises**[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=14)]

According to Visa Chief Enterprise Risk Officer Ellen Richey (2018):

"...no compromised entity has yet been found to be in compliance with PCI DSS at the time of a breach."[[22]](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard#cite_note-COMPUTERWORLD--Post-breach-PCI-22)

In 2008, a breach of [Heartland Payment Systems](https://en.wikipedia.org/wiki/Heartland_Payment_Systems#Security_breach), an organisation validated as compliant with PCI DSS, resulted in the compromising of one hundred million card numbers. Around this same time [Hannaford Brothers](https://en.wikipedia.org/wiki/Hannaford_Brothers_Company) and [TJX Companies](https://en.wikipedia.org/wiki/TJX_Companies), also validated as PCI DSS compliant, were similarly breached as a result of the alleged coordinated efforts of [Albert "Segvec" Gonzalez](https://en.wikipedia.org/wiki/Albert_Gonzalez) and two unnamed Russian hackers.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Assessments examine the compliance of merchants and services providers with the PCI DSS at a specific point in time and frequently utilize a sampling methodology to allow compliance to be demonstrated through representative systems and processes. It is the responsibility of the merchant and service provider to achieve, demonstrate, and maintain their compliance at all times both throughout the annual validation/assessment cycle and across all systems and processes in their entirety. Although it could be that a breakdown in merchant and service provider compliance with the written standard was to blame for the breaches, Hannaford Brothers had received its PCI DSS compliance validation one day after it had been made aware of a two-month-long compromise of its internal systems. The failure of this to be identified by the assessor suggests that incompetent verification of compliance undermines the security of the standard.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Other criticism lies in that compliance validation is required only for Level 1-3 merchants and may be optional for Level 4 depending on the card brand and acquirer. Visa's compliance validation details for merchants state that level 4 merchants compliance validation requirements are set by the acquirer, Visa level 4 merchants are "Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually". At the same time over 80% of payment card compromises between 2005 and 2007 affected Level 4 merchants; they handle 32% of transactions.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

See also[[edit](https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&action=edit&section=15)]

* [Penetration test](https://en.wikipedia.org/wiki/Penetration_test)
* [Vulnerability management](https://en.wikipedia.org/wiki/Vulnerability_management)
* [Wireless LAN](https://en.wikipedia.org/wiki/Wireless_LAN)
* [Wireless security](https://en.wikipedia.org/wiki/Wireless_security)

About ISO Standard Industries: Manufacturing

International Organization for Standardization

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#mw-head)[Jump to search](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#p-search)

*"ISO" redirects here. For other uses, see*[*ISO (disambiguation)*](https://en.wikipedia.org/wiki/ISO_(disambiguation))*.*

|  |  |
| --- | --- |
|  | This article **relies too much on**[**references**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability)**to**[**primary sources**](https://en.wikipedia.org/wiki/Wikipedia:No_original_research#Primary,_secondary_and_tertiary_sources). Please improve this article by adding [secondary or tertiary sources](https://en.wikipedia.org/wiki/Wikipedia:No_original_research#Primary,_secondary_and_tertiary_sources). *(July 2019) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

|  |  |
| --- | --- |
| **International Organization for Standardization** | |
| *Organisation internationale de normalisation* Международная организация по стандартизации | |
|  | |
| **Abbreviation** | ISO |
| **Formation** | 23 February 1947 |
| **Type** | [Non-governmental organization](https://en.wikipedia.org/wiki/Non-governmental_organization) |
| **Purpose** | [International standardization](https://en.wikipedia.org/wiki/International_standard) |
| **Headquarters** | [Geneva](https://en.wikipedia.org/wiki/Geneva), [Switzerland](https://en.wikipedia.org/wiki/Switzerland) |
| **Membership** | 164 members (40 correspondent and 4 subscriber)[[1]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISO_members-1) |
| **Official languages** | * [English](https://en.wikipedia.org/wiki/English_language) * [French](https://en.wikipedia.org/wiki/French_language) * [Russian](https://en.wikipedia.org/wiki/Russian_language)[[2]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-languages-2) |
| **President** | John Walter |
| **Website** | [iso.org](https://iso.org/) [Edit this at Wikidata](https://www.wikidata.org/wiki/Q15028#P856) |

The **International Organization for Standardization** (**ISO**; [/ˈaɪsoʊ/](https://en.wikipedia.org/wiki/Help:IPA/English)) is an [international standard](https://en.wikipedia.org/wiki/International_standard)-setting body composed of representatives from various national [standards organizations](https://en.wikipedia.org/wiki/Standards_organization).

Founded on 23 February 1947, the organization promotes worldwide proprietary, industrial, and commercial [standards](https://en.wikipedia.org/wiki/International_standard). It is headquartered in [Geneva](https://en.wikipedia.org/wiki/Geneva), Switzerland,[[3]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-About_ISO-3) and works in 164 countries.[[1]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISO_members-1)

It was one of the first organizations granted [general consultative status with the United Nations Economic and Social Council](https://en.wikipedia.org/wiki/List_of_organizations_with_consultative_status_to_the_United_Nations_Economic_and_Social_Council).



**Contents**

* [1Overview](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Overview)
* [2History](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#History)
* [3Language use](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Language_use)
* [4Name and abbreviations](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Name_and_abbreviations)
* [5Structure](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Structure)
  + [5.1IEC joint committees](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#IEC_joint_committees)
    - [5.1.1ISO/IEC JTC 1](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#ISO/IEC_JTC_1)
    - [5.1.2ISO/IEC JTC 2](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#ISO/IEC_JTC_2)
* [6Membership](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Membership)
* [7Financing](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Financing)
* [8International Standards and other publications](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#International_Standards_and_other_publications)
  + [8.1Document copyright](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Document_copyright)
* [9Standardization process](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Standardization_process)
* [10Products named after ISO](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Products_named_after_ISO)
* [11Criticism and laments](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Criticism_and_laments)
* [12See also](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#See_also)
* [13References](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#References)
* [14Further reading](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Further_reading)
* [15External links](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#External_links)

Overview[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=1)]

The International Organization for Standardization is an independent, non-governmental organization, the members of which are the standards organizations of the 164 member countries.[[1]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISO_members-1) It is the world's largest developer of voluntary international standards and it facilitates world trade by providing common standards among nations. More than twenty thousand standards have been set, covering everything from manufactured products and technology to food safety, agriculture, and healthcare.[[3]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-About_ISO-3)

Use of the standards aids in the creation of products and services that are safe, reliable, and of good quality. The standards help businesses increase productivity while minimizing errors and waste. By enabling products from different markets to be directly compared, they facilitate companies in entering new markets and assist in the development of global trade on a fair basis. The standards also serve to safeguard consumers and the end-users of products and services, ensuring that certified products conform to the minimum standards set internationally.[[3]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-About_ISO-3)

History[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=2)]

[](https://en.wikipedia.org/wiki/File:Memory_plaque_of_founding_ISA_in_Prague_cropped.jpg)

Plaque marking the building in [Prague](https://en.wikipedia.org/wiki/Prague) where the ISO predecessor, the ISA, was founded

The organization today known as ISO, began in the 1920s as the International Federation of the National Standardizing Associations (ISA). It was suspended in 1942 during [World War II](https://en.wikipedia.org/wiki/World_War_II),[[4]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-Brief_history-4) but after the war ISA was approached by the recently-formed United Nations Standards Coordinating Committee (UNSCC) with a proposal to form a new global standards body. In October 1946, ISA and UNSCC delegates from 25 countries met in London and agreed to join forces to create the new International Organization for Standardization. The new organization officially began operations in February 1947.[[5]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-50_years-5)

Language use[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=3)]

The three official languages of the ISO are [English](https://en.wikipedia.org/wiki/English_language) (with [Oxford spelling](https://en.wikipedia.org/wiki/Oxford_spelling)), [French](https://en.wikipedia.org/wiki/French_language), and [Russian](https://en.wikipedia.org/wiki/Russian_language).[[2]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-languages-2)

Name and abbreviations[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=4)]

The name of the organization in French is *Organisation internationale de normalisation*, and in Russian, Международная организация по стандартизации (*Mezhdunarodnaya organizatsiya po standartizatsii*). *ISO* is not an [acronym](https://en.wikipedia.org/wiki/Acronym). The organization adopted *ISO* as its abbreviated name in reference to the Greek word *isos* (ίσος, meaning "equal"),[[6]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-about_iso-6) as its name in the three official languages would have had different acronyms. During the founding meetings of the new organization, the Greek word explanation was not invoked, so this meaning may have been made public later.[[7]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso_name-7)

ISO gives this explanation of the name: "Because 'International Organization for Standardization' would have different acronyms in different languages (IOS in English, OIN in French), our founders decided to give it the short form *ISO*. *ISO* is derived from the Greek *isos*, meaning equal. Whatever the country, whatever the language, the short form of our name is always *ISO*."[[8]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-8)

Both the name *ISO* and the ISO logo are registered trademarks and their use is restricted.[[9]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso_logo-9)

Structure[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=5)]

ISO is a voluntary organization whose members are recognized authorities on standards, each one representing one country. Members meet annually at a General Assembly to discuss the strategic objectives of ISO. The organization is coordinated by a central secretariat based in [Geneva](https://en.wikipedia.org/wiki/Geneva).[[10]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISOStructureAndGovernance-10)

A council with a rotating membership of 20 member bodies provides guidance and governance, including setting the annual budget of the central secretariat.[[10]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISOStructureAndGovernance-10)[[11]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-tech_ctte_list-11)

The technical management board is responsible for more than 250 [technical committees](https://en.wikipedia.org/wiki/List_of_International_Organization_for_Standardization_technical_committees), who develop the ISO standards.[[10]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISOStructureAndGovernance-10)[[12]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso_technical_ctte-12)[[13]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-develops-13)[[14]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-governance-14)

**IEC joint committees**[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=6)]

ISO has formed two joint committees with the [International Electrotechnical Commission](https://en.wikipedia.org/wiki/International_Electrotechnical_Commission) (IEC) to develop standards and terminology in the areas of electrical and electronic related technologies.

**ISO/IEC JTC 1**[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=7)]

*Main article:*[*ISO/IEC JTC 1*](https://en.wikipedia.org/wiki/ISO/IEC_JTC_1)

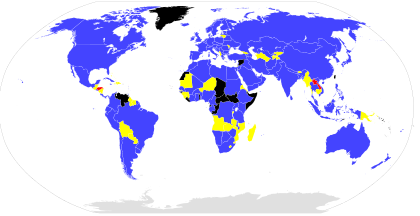
ISO/IEC Joint Technical Committee 1 (JTC 1) was created in 1987 to "[d]evelop, maintain, promote and facilitate IT standards",[[15]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-jtc1_home-15) where IT refers to information technology.

**ISO/IEC JTC 2**[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=8)]

ISO/IEC Joint Technical Committee 2 (JTC 2) was created in 2009 for the purpose of "[s]tandardization in the field of energy efficiency and renewable energy sources".[[16]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso_list_tech-16)

Membership[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=9)]

*Further information:*[*Countries in the International Organization for Standardization*](https://en.wikipedia.org/wiki/Countries_in_the_International_Organization_for_Standardization)

[](https://en.wikipedia.org/wiki/File:ISO_Members.svg)

  ISO member countries with a national standards body and ISO voting rights

  Correspondent members (countries without a national standards body)

  Subscriber members (countries with small economies)

ISO has 164 [national members](https://en.wikipedia.org/wiki/Countries_in_International_Organization_for_Standardization).[[1]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISO_members-1)

ISO has three membership categories,[[1]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISO_members-1)

* *Member bodies* are national bodies considered the most representative standards body in each country. These are the only members of ISO that have voting rights.
* *Correspondent members* are countries that do not have their own standards organization. These members are informed about the work of ISO, but do not participate in standards promulgation.
* *Subscriber members* are countries with small economies. They pay reduced membership fees, but can follow the development of standards.

Participating members are called "P" members, as opposed to observing members, who are called "O" members.

Financing[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=10)]

ISO is funded by a combination of:[[17]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso_general-17)

* Organizations that manage the specific projects or loan experts to participate in the technical work
* Subscriptions from member bodies, whose subscriptions are in proportion to each country's [gross national product](https://en.wikipedia.org/wiki/Gross_national_product) and trade figures
* Sale of standards

International Standards and other publications[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=11)]

*See also:*[*List of International Organization for Standardization standards*](https://en.wikipedia.org/wiki/List_of_International_Organization_for_Standardization_standards)

International standards are the main products of ISO. It also publishes technical reports, technical specifications, publicly available specifications, technical [corrigenda](https://en.wikipedia.org/wiki/Erratum), and guides.[[18]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISOUS95IECUS95directives2004-18)[[19]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-directives-19)

**International standards**

These are designated using the format *ISO[/IEC] [/ASTM] [IS] nnnnn[-p]:[yyyy] Title*, where *nnnnn* is the number of the standard, *p* is an optional part number, *yyyy* is the year published, and *Title* describes the subject. *IEC* for [*International Electrotechnical Commission*](https://en.wikipedia.org/wiki/International_Electrotechnical_Commission) is included if the standard results from the work of ISO/IEC JTC1 (the ISO/IEC Joint Technical Committee). *ASTM* (American Society for Testing and Materials) is used for standards developed in cooperation with [ASTM International](https://en.wikipedia.org/wiki/ASTM_International). *yyyy* and *IS* are not used for an incomplete or unpublished standard and, under some circumstances, may be left off the title of a published work.

**Technical reports**

These are issued when a technical committee or subcommittee has collected data of a different kind from that normally published as an International Standard,[[18]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISOUS95IECUS95directives2004-18) such as references and explanations. The naming conventions for these are the same as for standards, except *TR* prepended instead of *IS* in the report's name.

For example:

* ISO/IEC TR 17799:2000 Code of Practice for Information Security Management
* ISO/TR 19033:2000 Technical product documentation — Metadata for construction documentation

**Technical and publicly available specifications**

Technical specifications may be produced when "the subject in question is still under development or where for any other reason there is the future but not immediate possibility of an agreement to publish an International Standard". A publicly available specification is usually "an intermediate specification, published prior to the development of a full International Standard, or, in IEC may be a 'dual logo' publication published in collaboration with an external organization".[[18]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISOUS95IECUS95directives2004-18) By convention, both types of specification are named in a manner similar to the organization's technical reports.

For example:

* ISO/TS 16952-1:2006 Technical product documentation — Reference designation system — Part 1: General application rules
* ISO/PAS 11154:2006 Road vehicles — Roof load carriers

**Technical corrigenda**

ISO also sometimes issues "technical corrigenda" (where "corrigenda" is the plural of [corrigendum](https://en.wikipedia.org/wiki/Erratum)). These are amendments made to existing standards due to minor technical flaws, usability improvements, or limited-applicability extensions. They are generally issued with the expectation that the affected standard will be updated or withdrawn at its next scheduled review.[[18]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISOUS95IECUS95directives2004-18)

**ISO guides**

These are meta-standards covering "matters related to international standardization".[[18]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-ISOUS95IECUS95directives2004-18) They are named using the format *"ISO[/IEC] Guide N:yyyy: Title"*.

For example:

* ISO/IEC Guide 2:2004 Standardization and related activities — General vocabulary
* ISO/IEC Guide 65:1996 General requirements for bodies operating product certification

**Document copyright**[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=12)]

ISO documents are copyright and ISO charges for most copies. It does not, however, charge for most draft copies of documents in electronic format. Although they are useful, care must be taken using these drafts as there is the possibility of substantial change before they become finalized as standards. Some standards by ISO and its official U.S. representative (and, via the U.S. National Committee, the [International Electrotechnical Commission](https://en.wikipedia.org/wiki/International_Electrotechnical_Commission)) are made freely available.[[20]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-FreelyAvailableStandards-20)[[21]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-free_ansi-21)

Standardization process[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=13)]

A standard published by ISO/IEC is the last stage of a long process that commonly starts with the proposal of new work within a committee. Some abbreviations used for marking a standard with its status are:[[22]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-about-mpeg-22)[[23]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-stages-codes-23)[[24]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-stages-24)[[25]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-acronyms-committees-25)[[26]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-directives-procedures-26)[[27]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-abbr-27)[[28]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-us-tag-committee-28)

* PWI – Preliminary Work Item
* NP or NWIP – New Proposal / New Work Item Proposal (e.g., ISO/IEC NP 23007)
* AWI – Approved new Work Item (e.g., ISO/IEC AWI 15444-14)
* WD – Working Draft (e.g., ISO/IEC WD 27032)
* CD – Committee Draft (e.g., ISO/IEC CD 23000-5)
* FCD – Final Committee Draft (e.g., ISO/IEC FCD 23000-12)
* DIS – Draft International Standard (e.g., ISO/IEC DIS 14297)
* FDIS – Final Draft International Standard (e.g., ISO/IEC FDIS 27003)
* PRF – Proof of a new International Standard (e.g., ISO/IEC PRF 18018)
* IS – International Standard (e.g., ISO/IEC 13818-1:2007)

Abbreviations used for amendments are:[[22]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-about-mpeg-22)[[23]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-stages-codes-23)[[24]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-stages-24)[[25]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-acronyms-committees-25)[[26]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-directives-procedures-26)[[27]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-abbr-27)[[28]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-us-tag-committee-28)[[29]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-tr-ts-2009-29)

* NP Amd – New Proposal Amendment (e.g., ISO/IEC 15444-2:2004/NP Amd 3)
* AWI Amd – Approved new Work Item Amendment (e.g., ISO/IEC 14492:2001/AWI Amd 4)
* WD Amd – Working Draft Amendment (e.g., ISO 11092:1993/WD Amd 1)
* CD Amd / PDAmd – Committee Draft Amendment / Proposed Draft Amendment (e.g., ISO/IEC 13818-1:2007/CD Amd 6)
* FPDAmd / DAM (DAmd) – Final Proposed Draft Amendment / Draft Amendment (e.g., ISO/IEC 14496-14:2003/FPDAmd 1)
* FDAM (FDAmd) – Final Draft Amendment (e.g., ISO/IEC 13818-1:2007/FDAmd 4)
* PRF Amd – (e.g., ISO 12639:2004/PRF Amd 1)
* Amd – Amendment (e.g., ISO/IEC 13818-1:2007/Amd 1:2007)

Other abbreviations are:[[26]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-directives-procedures-26)[[27]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-abbr-27)[[29]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-tr-ts-2009-29)[[30]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-deliverables-30)

* TR – Technical Report (e.g., ISO/IEC TR 19791:2006)
* DTR – Draft Technical Report (e.g., ISO/IEC DTR 19791)
* TS – Technical Specification (e.g., ISO/TS 16949:2009)
* DTS – Draft Technical Specification (e.g., ISO/DTS 11602-1)
* PAS – Publicly Available Specification
* TTA – Technology Trends Assessment (e.g., ISO/TTA 1:1994)
* IWA – International Workshop Agreement (e.g., IWA 1:2005)
* Cor – Technical Corrigendum (e.g., ISO/IEC 13818-1:2007/Cor 1:2008)
* Guide – a guidance to technical committees for the preparation of standards

International Standards are developed by ISO technical committees (TC) and subcommittees (SC) by a process with six steps:[[24]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-stages-24)[[31]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-directives-part1-31)

* Stage 1: Proposal stage
* Stage 2: Preparatory stage
* Stage 3: Committee stage
* Stage 4: Enquiry stage
* Stage 5: Approval stage
* Stage 6: Publication stage

The TC/SC may set up [working groups](https://en.wikipedia.org/wiki/Working_group) (WG) of experts for the preparation of a working drafts. Subcommittees may have several working groups, which may have several Sub Groups (SG).[[32]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-wg11-structure-32)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stages in the development process of an ISO standard**[[23]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-stages-codes-23)[[24]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-stages-24)[[25]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-acronyms-committees-25)[[28]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-us-tag-committee-28)[[31]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-directives-part1-31)[[29]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-tr-ts-2009-29) | | | | |
| **Stage code** | **Stage** | **Associated document name** | **Abbreviations** | * **Description** * **Notes** |
| 00 | Preliminary | Preliminary work item | PWI |  |
| 10 | Proposal | New work item proposal | * NP or NWIP * NP Amd/TR/TS/IWA |  |
| 20 | Preparatory | Working draft or drafts | * AWI * AWI Amd/TR/TS * WD * WD Amd/TR/TS |  |
| 30 | Committee | Committee draft or drafts | * CD * CD Amd/Cor/TR/TS * PDAmd (PDAM) * PDTR * PDTS |  |
| 40 | Enquiry | Enquiry draft | * DIS * FCD * FPDAmd * DAmd (DAM) * FPDISP * DTR * DTS | (CDV in IEC) |
| 50 | Approval | Final draft | * FDIS * FDAmd (FDAM) * PRF * PRF Amd/TTA/TR/TS/Suppl * FDTR |  |
| 60 | Publication | International Standard | * ISO * TR * TS * IWA * Amd * Cor |  |
| 90 | Review |  |  |
| 95 | Withdrawal |  |  |  |

It is possible to omit certain stages, if there is a document with a certain degree of maturity at the start of a standardization project, for example, a standard developed by another organization. ISO/IEC directives also allow the so-called "Fast-track procedure". In this procedure a document is submitted directly for approval as a draft International Standard (DIS) to the ISO member bodies or as a final draft International Standard (FDIS), if the document was developed by an international standardizing body recognized by the ISO Council.[[24]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-stages-24)

The first step—a proposal of work (New Proposal) is approved at the relevant subcommittee or technical committee (e.g., SC29 and JTC1 respectively in the case of [Moving Picture Experts Group](https://en.wikipedia.org/wiki/Moving_Picture_Experts_Group) – ISO/IEC JTC1/SC29/WG11). A working group (WG) of experts is set up by the TC/SC for the preparation of a working draft. When the scope of a new work is sufficiently clarified, some of the working groups (e.g., MPEG) usually make open request for proposals—known as a "call for proposals". The first document that is produced, for example, for audio and video coding standards is called a verification model (VM) (previously also called a "simulation and test model"). When a sufficient confidence in the stability of the standard under development is reached, a working draft (WD) is produced. This is in the form of a standard, but is kept internal to working group for revision. When a working draft is sufficiently solid and the working group is satisfied that it has developed the best technical solution to the problem being addressed, it becomes a committee draft (CD). If it is required, it is then sent to the P-members of the TC/SC (national bodies) for ballot.

The committee draft becomes final committee draft (FCD) if the number of positive votes exceeds the quorum. Successive committee drafts may be considered until consensus is reached on the technical content. When consensus is reached, the text is finalized for submission as a draft International Standard (DIS). Then the text is submitted to national bodies for voting and comment within a period of five months. It is approved for submission as a final draft International Standard (FDIS) if a two-thirds majority of the P-members of the TC/SC are in favour and if not more than one-quarter of the total number of votes cast are negative. ISO will then hold a ballot with National Bodies where no technical changes are allowed (yes/no ballot), within a period of two months. It is approved as an International Standard (IS) if a two-thirds majority of the P-members of the TC/SC is in favour and not more than one-quarter of the total number of votes cast are negative. After approval, only minor editorial changes are introduced into the final text. The final text is sent to the ISO central secretariat, which publishes it as the International Standard.[[22]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-about-mpeg-22)[[24]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso-stages-24)

Products named after ISO[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=14)]

On occasion, the fact that many of the ISO-created standards are ubiquitous, has led to common use of "ISO" to describe the product that conforms to a standard. Some examples of this are:

* [Disk images](https://en.wikipedia.org/wiki/Disk_images) end in the [file extension](https://en.wikipedia.org/wiki/File_extension) "[ISO](https://en.wikipedia.org/wiki/ISO_image)" to signify that they are using the [ISO 9660](https://en.wikipedia.org/wiki/ISO_9660) standard file system as opposed to another file system—hence Discs images commonly are referred to as "ISOs".
* The sensitivity of a photographic film to light (its "[film speed](https://en.wikipedia.org/wiki/Film_speed)") is described by [ISO 6](https://en.wikipedia.org/wiki/ISO_6), [ISO 2240](https://en.wikipedia.org/wiki/ISO_2240) and [ISO 5800](https://en.wikipedia.org/wiki/ISO_5800). Hence, the speed of the film often is referred to by its ISO number.
* As it was originally defined in ISO 518, the flash [hot shoe](https://en.wikipedia.org/wiki/Hot_shoe) found on cameras often is called the "ISO shoe".
* [ISO 11783](https://en.wikipedia.org/wiki/ISO_11783), which is marketed as ISOBUS.
* [ISO 13216](https://en.wikipedia.org/wiki/ISO_13216), which is marketed as ISOFIX.

Criticism and laments[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=15)]

With the exception of a small number of isolated standards,[[20]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-FreelyAvailableStandards-20) normally ISO standards are not available free of charge, but for a purchase fee,[[33]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-iso_shopFAQ-33) which has been seen by some as unaffordable by small [open source](https://en.wikipedia.org/wiki/Open-source_model) projects.[[34]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-oreilly2007-34)

The [ISO/IEC JTC1](https://en.wikipedia.org/wiki/ISO/IEC_JTC1) fast-track procedures ("Fast-track" as used by [OOXML](https://en.wikipedia.org/wiki/Office_Open_XML) and "PAS" as used by [OpenDocument](https://en.wikipedia.org/wiki/OpenDocument)) have garnered criticism in relation to the [standardization of Office Open XML](https://en.wikipedia.org/wiki/Standardization_of_Office_Open_XML) (ISO/IEC 29500). Martin Bryan, outgoing convenor of [ISO/IEC JTC1/SC34](https://en.wikipedia.org/wiki/ISO/IEC_JTC1/SC34) WG1, is quoted as saying:[[35]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-jtc1_sc34_0940-35)

I would recommend my successor that it is perhaps time to pass WG1’s outstanding standards over to OASIS, where they can get approval in less than a year and then do a PAS submission to ISO, which will get a lot more attention and be approved much faster than standards currently can be within WG1.

The disparity of rules for PAS, Fast-Track and ISO committee generated standards is fast making ISO a laughing stock in IT circles. The days of open standards development are fast disappearing. Instead we are getting "standardization by corporation".

The computer security entrepreneur and [Ubuntu](https://en.wikipedia.org/wiki/Ubuntu_(operating_system)) founder, [Mark Shuttleworth](https://en.wikipedia.org/wiki/Mark_Shuttleworth), commented on the [Standardization of Office Open XML](https://en.wikipedia.org/wiki/Standardization_of_Office_Open_XML) process by saying: "I think it de-values the confidence people have in the standards setting process", and alleged that ISO did not carry out its responsibility. He also noted that [Microsoft](https://en.wikipedia.org/wiki/Microsoft) had intensely lobbied many countries that traditionally had not participated in ISO and stacked technical committees with Microsoft employees, solution providers, and resellers sympathetic to Office Open XML:[[36]](https://en.wikipedia.org/wiki/International_Organization_for_Standardization#cite_note-zdnet_2222-36)

When you have a process built on trust and when that trust is abused, ISO should halt the process... ISO is an engineering [old boys club](https://en.wikipedia.org/wiki/Old_boy_network) and these things are boring so you have to have a lot of passion … then suddenly you have an investment of a lot of money and lobbying and you get artificial results. The process is not set up to deal with intensive corporate [lobbying](https://en.wikipedia.org/wiki/Lobbying) and so you end up with something being a standard that is not clear.

See also[[edit](https://en.wikipedia.org/w/index.php?title=International_Organization_for_Standardization&action=edit&section=16)]

* [AP Stylebook](https://en.wikipedia.org/wiki/AP_Stylebook) – book on English usage by Associated Press
* [Countries in the International Organization for Standardization](https://en.wikipedia.org/wiki/Countries_in_the_International_Organization_for_Standardization)
* [Ecma International](https://en.wikipedia.org/wiki/Ecma_International) – Standards organization for information and communication systems
* [Engelbert Pigal](https://en.wikipedia.org/wiki/Engelbert_Pigal)
* [European Committee for Standardization](https://en.wikipedia.org/wiki/European_Committee_for_Standardization) (CEN)
* [Global Reporting Initiative](https://en.wikipedia.org/wiki/Global_Reporting_Initiative) for sustainability information and linking up with reporting on their 17#[GlobalGoals](https://en.wikipedia.org/wiki/GlobalGoals) indicators
* [GOST](https://en.wikipedia.org/wiki/GOST), a set of technical standards maintained by the Euro-Asian Council for Standardization, Metrology, and Certification
* [IEEE Standards Association](https://en.wikipedia.org/wiki/IEEE_Standards_Association)
* [Institute of Environmental Sciences and Technology](https://en.wikipedia.org/wiki/Institute_of_Environmental_Sciences_and_Technology)
* [Interface 2010](https://en.wikipedia.org/wiki/Interface_2010), the Interface Marketing Supplier Integration Institute
* [International Classification for Standards](https://en.wikipedia.org/wiki/International_Classification_for_Standards)
* [The International Customer Service Institute](https://en.wikipedia.org/wiki/The_International_Customer_Service_Institute)
* [International Electrotechnical Commission](https://en.wikipedia.org/wiki/International_Electrotechnical_Commission) (IEC)
* [International healthcare accreditation](https://en.wikipedia.org/wiki/International_healthcare_accreditation)
* [International Telecommunication Union](https://en.wikipedia.org/wiki/International_Telecommunication_Union) – Specialized agency of the United Nations
* [Internet Engineering Task Force](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force)
* [List of International Organization for Standardization standards](https://en.wikipedia.org/wiki/List_of_International_Organization_for_Standardization_standards) – Wikipedia list article
* [Standardization](https://en.wikipedia.org/wiki/Standardization) – Implementation of technical standards based on the consensus of different parties
* [Standards organization](https://en.wikipedia.org/wiki/Standards_organization) – Organization that develops standards
* [Terminology planning policy](https://en.wikipedia.org/wiki/Terminology_planning_policy)
* ISO divisions
  + [ISO/TC 37](https://en.wikipedia.org/wiki/ISO/TC_37) "Terminology and other language and content resources", a fundamental ISO standardization committee
  + [ISO/TC 68](https://en.wikipedia.org/wiki/ISO/TC_68)
  + [ISO TC 46/SC 9](https://en.wikipedia.org/wiki/ISO_TC_46/SC_9)
  + [ISO/TC 176](https://en.wikipedia.org/wiki/ISO/TC_176)
  + [ISO/TC 211 Geographic information/Geomatics](https://en.wikipedia.org/wiki/ISO/TC_211_Geographic_information/Geomatics)
  + [ISO/TC 215](https://en.wikipedia.org/wiki/ISO/TC_215)
  + [ISO/TC 223](https://en.wikipedia.org/wiki/ISO/TC_223)
  + [ISO/TC 262](https://en.wikipedia.org/wiki/ISO/TC_262)
  + [ISO/TC 289](https://en.wikipedia.org/wiki/ISO/TC_289)
  + [ISO/TC 292](https://en.wikipedia.org/wiki/ISO/TC_292)

About ITAR Industries: Government Contractors Manufacturing

International Traffic in Arms Regulations

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#mw-head)[Jump to search](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#p-search)

*"ITAR" redirects here. For the Russian news agency, see*[*Information Telegraph Agency of Russia*](https://en.wikipedia.org/wiki/Information_Telegraph_Agency_of_Russia)*.*

**International Traffic in Arms Regulations** (**ITAR**) is a United States regulatory regime to restrict and control the export of defense and military related technologies to safeguard U.S. national security and further U.S. foreign policy objectives.[[1]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-1)

Defense-related articles and services on the [United States Munitions List](https://en.wikipedia.org/wiki/United_States_Munitions_List) (USML)[[2]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-2) are covered by the regulations, which implement the provisions of the [Arms Export Control Act](https://en.wikipedia.org/wiki/Arms_Export_Control_Act) (AECA), and are described in Title 22 (Foreign Relations), Chapter I ([Department of State](https://en.wikipedia.org/wiki/United_States_Department_of_State)), Subchapter M of the [Code of Federal Regulations](https://en.wikipedia.org/wiki/Code_of_Federal_Regulations). The Department of State [Directorate of Defense Trade Controls](https://en.wikipedia.org/wiki/Directorate_of_Defense_Trade_Controls) (DDTC) interprets and enforces ITAR. The related [Export Administration Regulations](https://en.wikipedia.org/wiki/Export_Administration_Regulations) (Code of Federal Regulations Title 15 chapter VII, subchapter C) are enforced and interpreted by the [Bureau of Industry and Security](https://en.wikipedia.org/wiki/Bureau_of_Industry_and_Security) in the Commerce Department. The [Department of Defense](https://en.wikipedia.org/wiki/United_States_Department_of_Defense) is also involved in the review and approval process. Physical enforcement of the ITAR (as well as all import and export laws of the United States) is performed by [Homeland Security](https://en.wikipedia.org/wiki/United_States_Department_of_Homeland_Security) Investigations Special Agents (formerly U.S. Customs) under [Immigration and Customs Enforcement](https://en.wikipedia.org/wiki/U.S._Immigration_and_Customs_Enforcement), an agency of the [Department of Homeland Security](https://en.wikipedia.org/wiki/United_States_Department_of_Homeland_Security). Additionally, Customs and Border Protection Officers, also under the Department of Homeland Security, inspect imports and exports at U.S. Border Crossings and International Airports and enforce import and export regulations.

For practical purposes, ITAR regulations dictate that information and material pertaining to defense and military related technologies (items listed on the U.S. Munitions List) may only be shared with [U.S. Persons](https://en.wikipedia.org/wiki/United_States_person) unless authorization from the Department of State is received or a special exemption is used.[[3]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-pmddtc.state.gov-3) U.S. Persons (including organizations; see [legal personality](https://en.wikipedia.org/wiki/Legal_personality)) can face heavy fines if they have, without authorization or the use of an exemption, provided foreign persons with access to ITAR-protected defense articles, services or technical data.[[4]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Consent-4)

The U.S. Munitions List changes over time. Until 1996–1997, ITAR classified strong [cryptography](https://en.wikipedia.org/wiki/Cryptography) as arms and prohibited their export from the U.S.[[5]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-5) Another change occurred as a result of [Space Systems/Loral](https://en.wikipedia.org/wiki/Space_Systems/Loral)'s conduct after the February 1996 failed launch of the [Intelsat 708](https://en.wikipedia.org/wiki/Intelsat_708) satellite. The Department of State charged [Space Systems/Loral](https://en.wikipedia.org/wiki/Space_Systems/Loral) with violating the [Arms Export Control Act](https://en.wikipedia.org/wiki/Arms_Export_Control_Act) and the ITAR.[[6]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-6)[[7]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-7) As a result, technology pertaining to [satellites](https://en.wikipedia.org/wiki/Satellites) and [launch vehicles](https://en.wikipedia.org/wiki/Launch_vehicle) became more carefully protected.

ITAR does not apply to information related to general scientific, mathematical or engineering principles that are commonly taught in schools and colleges or information that is in the public domain.[[8]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-ITAR-8):§ 120.10(5)[[8]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-ITAR-8):§ 120.11 Nor does it apply to general marketing information or basic system descriptions.[[8]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-ITAR-8):§ 120.10(5) Broad interpretations of these exceptions have faced several legal challenges. For example, college professors have been prosecuted for breaches of the AECA as a result of access to USML items by foreign graduate students[[9]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-9) and companies have been penalized for alleged breaches of the AECA for failing to properly remove USML items from material used to market defense articles.[[10]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-10) The U.S. Government has also taken action (albeit unsuccessfully) for the export of technical data that was allegedly already publicly available on the Internet.[[11]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-elb-1-11)[[12]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-12)[[13]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-13)[[14]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-14)

ITAR applies to items identified under the [Invention Secrecy Act](https://en.wikipedia.org/wiki/Invention_Secrecy_Act).



**Contents**

* [1History](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#History)
* [2Operation](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Operation)
  + [2.1Classification of Defense Articles](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Classification_of_Defense_Articles)
  + [2.2Registration](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Registration)
  + [2.3Exporting Defense Articles](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Exporting_Defense_Articles)
* [3Restrictions on Retransfer](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Restrictions_on_Retransfer)
* [4Restrictions on Retransfer to Dual Nationals and Third Country Nationals](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Restrictions_on_Retransfer_to_Dual_Nationals_and_Third_Country_Nationals)
* [5Enforcement](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Enforcement)
* [6Compliance](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Compliance)
* [7ITAR reform](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#ITAR_reform)
* [8Controversy](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Controversy)
  + [8.1Harm to U.S. commercial and academic interests](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Harm_to_U.S._commercial_and_academic_interests)
    - [8.1.1Academic work and the "Fundamental Research Exemption"](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Academic_work_and_the_%22Fundamental_Research_Exemption%22)
    - [8.1.2Effects on the U.S. space industry](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Effects_on_the_U.S._space_industry)
  + [8.2Registration fees](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Registration_fees)
  + [8.3Restrictions on foreign products](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Restrictions_on_foreign_products)
  + [8.4Restrictions on Dual and Third Country Nationals](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Restrictions_on_Dual_and_Third_Country_Nationals)
  + [8.5ITAR and information technology](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#ITAR_and_information_technology)
  + [8.6Exemptions and treaties](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Exemptions_and_treaties)
  + [8.7Satellite components](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#Satellite_components)
* [9See also](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#See_also)
* [10References](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#References)
* [11External links](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#External_links)

History[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=1)]

The AECA and ITAR were enacted in 1976 during the [Cold War](https://en.wikipedia.org/wiki/Cold_War) with USSR and were intended to implement unilateral arms export controls that reflected those imposed on [Eastern Bloc](https://en.wikipedia.org/wiki/Eastern_Bloc) countries by the multilateral [Coordinating Committee for Multilateral Export Controls](https://en.wikipedia.org/wiki/Coordinating_Committee_for_Multilateral_Export_Controls).[[15]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-15)[[16]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-16)

U.S. Government enforcement activities have increased dramatically since 1999,[[17]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-17) when the U.S. Department of State took over export regulations for satellites.[[18]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-economist-18) The U.S. Department of State has published 29 instances of Consent Agreements (agreements entered into by parties charged with breaches of ITAR) since 1999.[[4]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Consent-4) This compares to 12 Consent Agreements in the preceding 22 years.[[4]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Consent-4) ITAR's prominence has also increased as its implications for foreign parties that handle USML items have become better understood (see "Controversy" below).

ITAR's impact of increased regulations also meant America's worldwide market share in satellite technology declined from 83 percent to 50 percent in 2008, states [The Economist](https://en.wikipedia.org/wiki/The_Economist), which cited a report from [Space Review](https://en.wikipedia.org/wiki/Space_Review).[[18]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-economist-18) In early 2013 legislation was passed allowing the removal of satellite technology from ITAR regulation.[[19]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-sfn-20130103-19)

Operation[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=2)]

**Classification of Defense Articles**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=3)]

The ITAR regulate defense articles and defense services.

Defense articles can be broken down into two categories: (a) physical items (often referred to as "commodities") and (b) technical data. The ITAR contain a list of defense articles called the US Munitions List ("USML"), which can be found at [22 CFR §121.1](https://www.ecfr.gov/cgi-bin/text-idx?SID=86008bdffd1fb2e79cc5df41a180750a&node=22:1.0.1.13.58&rgn=div5). The USML is broken down into the following categories:

I:   Firearms, Close Assault Weapons and Combat Shotguns

II:   Materials, Chemicals, Microorganisms, and Toxins

III:   Ammunition/Ordnance

IV:   Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines

V:   Explosives and Energetic Materials, Propellants, Incendiary Agents and Their Constituents

VI:   Vessels of War and Special Naval Equipment

VII:   Tanks and Military Vehicles

VIII:   Aircraft and Associated Equipment

IX:   Military Training Equipment

X:   Protective Personnel Equipment

XI:   Military Electronics

XII:   Fire Control, Range Finder, Optical and Guidance and Control Equipment

XIII:   Auxiliary Military Equipment

XIV:   Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment

XV:   Spacecraft Systems and Associated Equipment

XVI:   Nuclear Weapons, Design and Testing Related Items

XVII:  Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated

XVIII: Directed Energy Weapons

XX:   Submersible Vessels, Oceanographic and Associated Equipment

XXI:   Articles, Technical Data, and Defense Services Not Otherwise Enumerated

For example, an M4 rifle would be found at Category I paragraph (b):

\*(b) Fully automatic firearms to .50 caliber inclusive (12.7 mm).

A flash suppressor for the M4 rifle then follows in paragraph (e):

\*(e) Silencers, mufflers, sound and flash suppressors for the articles in (a) through (d) of this category and their specifically designed, modified or adapted components and parts.

Components, parts, and accessories for the M4 rifle are in paragraph (h):

(h) Components, parts, accessories and attachments for the articles in paragraphs (a) through (g) of this category.

Finally, technical data and defense services relating to the rifle are in paragraph (i):

(i) Technical data (as defined in §120.10 of this subchapter) and defense services (as defined in §120.9 of this subchapter) directly related to the defense articles described in paragraphs (a) through (h) of this category. Technical data directly related to the manufacture or production of any defense articles described elsewhere in this category that are designated as Significant Military Equipment (SME) shall itself be designated SME.

Technical data is defined in the ITAR at [22 CFR §120.10](https://www.ecfr.gov/cgi-bin/text-idx?SID=7eb11c7f9b0a7712135f1c6fefbcfc2e&mc=true&node=pt22.1.120&rgn=div5#se22.1.120_110) as:

(1) Information, other than software as defined in §120.10(a)(4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.

(2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List;

(3) Information covered by an invention secrecy order; or

(4) Software (*see* §120.45(f)) directly related to defense articles.[[20]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-20)

**Registration**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=4)]

All U.S. manufacturers, exporters, and brokers of defense articles, defense services, or related technical data, as defined on the USML, are required to register with U.S. Department of State. Registration is primarily a means to provide the U.S. Government with necessary information on who is involved in certain manufacturing and exporting activities. Registration does not confer any export rights or privileges, but is a precondition for the issuance of any license or other approval for export.[[21]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-21) Registration fees start at US$2,250 per year.[[22]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-22)

**Exporting Defense Articles**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=5)]

Under ITAR, a "US person" who wants to export USML items to a "foreign person" must obtain authorization from the U.S. Department of State before the export can take place.[[3]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-pmddtc.state.gov-3)

A "U.S. person" can be

* a [U.S. citizen](https://en.wikipedia.org/wiki/United_States_nationality_law);
* a [permanent resident](https://en.wikipedia.org/wiki/Permanent_resident) who does not work for a foreign company, a foreign government, or a foreign governmental agency/organization;
* a political asylee;
* a part of the U.S. government, or
* a corporation, business, organization, or group that is incorporated in the United States under U.S. law.[[8]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-ITAR-8):§ 120.15

A foreign person is any person who is not a lawful permanent resident of the U.S. and includes foreign governments and organizations.[[8]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-ITAR-8):§ 120.16 This means that, for example a foreign person who is visiting the U.S. will remain a foreign person for the purposes of ITAR and any export of USML items to them inside the U.S. must be subject to an export authorization. This is similar to the concept of "Deemed Exports" used by the [Bureau of Industry and Security](https://en.wikipedia.org/wiki/Bureau_of_Industry_and_Security) within the [Department of Commerce](https://en.wikipedia.org/wiki/Department_of_Commerce) in administration of the [Export Administration Regulations](https://en.wikipedia.org/wiki/Export_Administration_Act_of_1979) although the Department of State does not use the term "Deemed Export"[[23]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-23) (see also "Restrictions on Dual and Third Country Nationals below").

The export authorization may take the form of:

* a [Foreign Military Sales](https://en.wikipedia.org/wiki/Foreign_Military_Sales) ("FMS") Case whereby the U.S. Government sells the USML items directly to a foreign government;[[24]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-24)[[25]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-25)
* an export license, such as a DSP-5 (Department of State Publication No. 5), which authorizes the temporary or permanent export of defense articles and/or technical data to a foreign person (but not technical assistance or defense services);[[26]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-26)
* a Warehouse and Distribution Agreement which is an agreement to establish a warehouse or distribution point abroad for defense articles to be exported from the United States for subsequent distribution to entities in an approved sales territory;[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27):9
* a Technical Assistance Agreement ("TAA") which authorizes a U.S. manufacturer/service provider to supply defense services to a foreign person (which could involve training or technical discussions regarding U.S. technology);[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27):8 or
* a Manufacturing License Agreement ("MLA") which authorises a U.S. manufacturer to supply manufacturing know-how related to defense articles to a foreign person.[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27)

Where the export authorization relates to USML items that are [classified information](https://en.wikipedia.org/wiki/Classified_information) or are identified as "Significant Military Equipment"[[8]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-ITAR-8):§ 120.7 on the USML, a DSP-83 Nontransfer and Use Certificate will also be required.[[8]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-ITAR-8):§ 123.10

Collaborative programs (also known as "Armaments Cooperative Projects" ("ACPs")) between the U.S. and foreign Governments (such as the [Joint Strike Fighter](https://en.wikipedia.org/wiki/Joint_Strike_Fighter)) may also authorize export of USML items (subject to strict controls).[[28]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-defence.gov.au-28)

Restrictions on Retransfer[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=6)]

ITAR also operates to prohibit the "Retransfer" (also called "Re-export") of items on the USML by foreign persons unless the Retransfer is specifically authorized under the relevant export authorization.

[](https://en.wikipedia.org/wiki/File:F-16_June_2008.jpg)

ITAR's restrictions on retransfer blocked Venezuela's threatened sale of used [F-16](https://en.wikipedia.org/wiki/F-16) aircraft to Iran in 2006.[[29]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-29)

The prohibition on Retransfer stems from the requirement for all export authorizations to include the statement that "[t]he technical data or defense service exported from the United States in furtherance of this agreement and any defense article which may be produced or manufactured from such technical data or defense service may not be transferred to a person in a third country or to a national of a third country except as specifically authorized in this agreement unless the prior written approval of the Department of State has been obtained."[[30]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-124.85-30)

This means that if, for example, a foreign person wants to Retransfer a USML item to another foreign person (such as a subcontractor), both foreign persons must be authorized under the relevant export authorization:

* where the export authorization is a FMS Case, the foreign government must have "Third Party Transfer Approval" from the U.S. Government;[[31]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-31)
* if the export authorization is an export license such as a DSP-5, all foreign parties must be named on the license (for example, some may be "intermediate consignees");[[32]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-32) and
* where the export authorization is a TAA or MLA, all foreign recipients must be named as parties to (or as "authorized sublicensees" under) the agreement.[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27):¶ 3.2

Where a foreign person requires access to USML items exported under a specific export authorization, but that foreign person is not authorized under the export authorization, the export authorization must be amended and re-approved by the U.S. Department of State.[[28]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-defence.gov.au-28) This can be a time-consuming process.[[28]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-defence.gov.au-28)

Restrictions on Retransfer to Dual Nationals and Third Country Nationals[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=7)]

ITAR treats access to USML items by "Dual-National" and "Third Country National" employees of a foreign organization as a Retransfer to the employees' other countries of nationality.[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27):¶ 3.9.b As a result, access to USML items by such employees must be specifically authorized under the relevant export authorization.[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27):¶ 3.9.c If access to USML items by Dual and Third Country National employees of a foreign organization is authorized, it only authorizes transfer to the employee. It does not authorize export to the employee's country of Dual or Third Nationality.[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27)

If a U.S. export authorization is silent as to access by Dual and Third Country National employees of a foreign party, the authorization has the effect of limiting access to employees who are nationals only of the country of their employer.[[30]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-124.85-30) This means that, for example, a TAA that includes a UK company as the foreign person, but which does not include clauses authorizing access by Dual and Third Country Nationals will limit access to USML items supplied under the TAA to employees of the UK company who are UK citizens only.

This can cause significant problems for foreign governments and organizations from countries with large [first generation immigrant](https://en.wikipedia.org/wiki/First_generation_immigrant) populations (which is discussed in more detail under "Controversy").[[33]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-abc.net.au-33) As a result, the U.S. Government and the [Australian Government](https://en.wikipedia.org/wiki/Australian_Government) have drawn attention to the importance for U.S. companies to consult closely with foreign persons who will be subject to a U.S. export authorization before it is submitted to the U.S. Department of State for approval.[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27):31[[34]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-34)

Clauses approved by the U.S. Department of State must be included in TAAs and MLAs in order to authorize access to USML items by Dual and Third Country National employees of foreign parties to the export authorization.[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27) These clauses will generally permit access by Dual and Third Country Nationals from [NATO](https://en.wikipedia.org/wiki/NATO), EU, Japan, Switzerland, New Zealand and Australia (subject to certain conditions).[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27) Employees of foreign persons holding Dual or Third Country Nationality from countries proscribed under ITAR 126.1, such as Vietnam, [The People's Republic of China](https://en.wikipedia.org/wiki/The_People%27s_Republic_of_China) ("PRC"), North Korea, Syria and Iran, will, as a general rule, not be authorized to have access to USML items.[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27):20 It is less-clear how Dual and Third Country Nationals are addressed in FMS Cases and export licenses such as DSP-5s.

Enforcement[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=8)]

The U.S. Government has substantially increased action against organizations and individuals responsible for breaches of ITAR since 1999. The most notable enforcement action was the $100M penalty applied to [ITT](https://en.wikipedia.org/wiki/ITT_Corporation) as a result of the unauthorized Retransfer of [night vision](https://en.wikipedia.org/wiki/Night_vision) technology to the PRC in 2007.[[35]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-ittcorp-35) Other major U.S. defense contractors penalized for alleged[[36]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Lockheed_Martin_Corporation-36) breaches of ITAR in recent years include (among others) [Lockheed Martin](https://en.wikipedia.org/wiki/Lockheed_Martin),[[37]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-37) [Motorola](https://en.wikipedia.org/wiki/Motorola),[[38]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-38) [Boeing](https://en.wikipedia.org/wiki/Boeing),[[39]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-39) [L-3 Communications](https://en.wikipedia.org/wiki/L-3_Communications),[[40]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-40) and [Northrop Grumman](https://en.wikipedia.org/wiki/Northrop_Grumman).[[41]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-41)

In most cases, penalties against corporate entities involve a mandatory compliance component requiring the entity to spend funds on compliance measures, including the appointment of "Internal Special Compliance Officers".[[36]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Lockheed_Martin_Corporation-36) Penalties may also require the party to submit to external audit. In serious cases, a party may be debarred from future exporting for a period of time.[[35]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-ittcorp-35)

U.S. Government policy also imposes a positive obligation on U.S. companies to fully disclose any breaches of ITAR to the U.S. Government.[[42]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-42) Failure to do so can significantly increase penalties applied by the U.S. Government.[[43]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-43)[[44]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-44):2

The U.S. Government:

* will also penalize U.S. companies for breaches of ITAR caused by their overseas subsidiaries;[[45]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-45)[[46]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-46)[[47]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-exportlawblog1-47)
* is critical of companies that have not implemented effective export compliance programs;[[48]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Qioptiq_ProposedChargingLetter_pp6-7-48)[[49]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-49) and
* treats breaches of ITAR as a [strict liability](https://en.wikipedia.org/wiki/Strict_liability) offence and will penalize a successor or purchaser of a company that has breached ITAR as though it was responsible for the breaches.[[47]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-exportlawblog1-47)[[50]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-50)

[](https://en.wikipedia.org/wiki/File:PEO_ANAVS-6_NVG.jpg)

The unauthorized export of night vision technology has been the subject of several enforcement actions by the U.S. Government.

The U.S. Government will also take action against individuals responsible for breaches of ITAR and such action can involve criminal penalties. Actions are often initiated by U.S. Immigrations and Customs Enforcement and include:

* the prosecution of Dr J Reece Roth of the University of Tennessee in 2008 for breaches of ITAR as a result of access to USML items by a PRC graduate student;[[51]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-51)
* the prosecution of Yen Ching Peng, a Taiwanese national, in the U.S. in 2008 for breaches of ITAR as a result of attempts to export [night vision](https://en.wikipedia.org/wiki/Night_vision) technology and [laser sights](https://en.wikipedia.org/wiki/Laser_sights) without the appropriate export authorizations;[[52]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-52)
* the indictment of 3 men, 2 U.S. nationals and a Vietnamese national, in 2008 on charges of illegally exporting [night vision](https://en.wikipedia.org/wiki/Night_vision) technology to Vietnam;[[53]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-53) and
* the prosecution of [Chi Mak](https://en.wikipedia.org/wiki/Chi_Mak) in 2007 as a result of (among other things) the attempted export of USML items to the PRC (Chi Mak was subsequently sentenced to 24 ½ years in Federal prison).[[54]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-54)

Since 1990, the U.S. Government has also operated the "Blue Lantern" end-use monitoring program.[[55]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-enduse12-55) Blue Lantern "monitors the end-use of commercially exported defense articles, defense services, and related technical data subject to licensing or other authorizations under section 38 of the AECA."[[55]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-enduse12-55) Blue Lantern checks are conducted following a careful selection process to identify transactions that appear most at risk for diversion or misuse.[[55]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-enduse12-55) Unfavorable Blue Lanterns are reviewed by DTCC's Enforcement Division. Where appropriate, parties involved in unfavorable Blue Lantern cases may be subject to civil enforcement actions or referred to law enforcement for criminal investigation.[[55]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-enduse12-55)

Compliance[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=9)]

Because failure to implement an effective export compliance program can be an exacerbating factor in the event of a breach of ITAR,[[48]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Qioptiq_ProposedChargingLetter_pp6-7-48) the U.S. Government encourages U.S. exporters to implement internal export compliance programs.[[56]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-56)[[57]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-57) The U.S. Government may also require U.S. exporters that are party to an export authorization to develop a "Technology Transfer Control Plan" specific to that export authorization.[[58]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-58)[[59]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-59)

Other countries also encourage their nationals who are using USML items to implement internal export compliance programs to address ITAR requirements. It is notable that the failure of overseas companies to implement ITAR compliance programs has been criticized by the U.S. Department of State.[[48]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Qioptiq_ProposedChargingLetter_pp6-7-48)

Companies in U.S. and Overseas are increasingly using the ERP software to track the ITAR controlled items through the Supply Chain.

ITAR reform[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=10)]

While political debate over the wisdom of placing all [satellite](https://en.wikipedia.org/wiki/Satellite) and [launch](https://en.wikipedia.org/wiki/Launch_vehicle) technology on the US Munitions List (USML) has been ongoing since the advent of ITAR regulation in 1999, there has been a shift in political opinion since 2007. In late 2012, the [US Congress](https://en.wikipedia.org/wiki/US_Congress) passed the [2013 defense authorization bill](https://en.wikipedia.org/wiki/National_Defense_Authorization_Act_for_Fiscal_Year_2013) which, if signed into law, will allow U.S. satellite manufacturers to "be more able to collaborate with international partners and [place] U.S. component makers on a more even footing in the global marketplace."[[60]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-aw20121224-60) The bill "allows the president to remove commercial satellites and components from the U.S. Munitions List (USML) and allows him to decide which satellite technologies are the most important to protect. The bill still restricts the export and transfer of technology to China, Cuba, Iran, North Korea, Sudan and Syria."[[60]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-aw20121224-60)

The political changes in 2012 came after several years of a gradual shift in thinking. In 2010, the Congress formally requested "an assessment of the national security risks of removing satellites and components from the USML. The study, known as the *1248 report*, was completed in April 2012.[[60]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-aw20121224-60)

While satellite technology had been subjected to ITAR since 1999, the U.S. had seen its share of global satellite manufacturing halved with, according to the [Aerospace Industries Association](https://en.wikipedia.org/wiki/Aerospace_Industries_Association), an estimated loss of $21 billion in revenue from 1999 to 2009.[[19]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-sfn-20130103-19)

Controversy[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=11)]

**Harm to U.S. commercial and academic interests**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=12)]

There is an open debate between the [Department of State](https://en.wikipedia.org/wiki/United_States_Department_of_State) and the industries and academia regulated by ITAR concerning how harmful the regulatory restrictions are for [U.S.](https://en.wikipedia.org/wiki/United_States)-[domiciled](https://en.wikipedia.org/wiki/Domicile_(law)) businesses and higher education institutions.

**Academic work and the "Fundamental Research Exemption"**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=13)]

Higher education institutions argue that ITAR prevents the best international students from studying and contributing in the United States, and prevents cooperation on certain types of international scientific projects.[[61]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-sattoday08-61)[[62]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-62) ITAR generally prohibits foreign persons from collaborating with US citizens on projects pertaining to items on the USML without export licensing, as such work can be construed to fall under one of the several enumerated definitions of "export," such as:[[63]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-eCFR-63)

* *"Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person"*
* *"Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad"*

Where the definition of "defense service" includes *"the furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles."*

The ITAR specifies that the products of "fundamental research" are not considered controlled "technical data," so long as they are published freely. Fundamental research is defined as university-based *"basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls."*[[63]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-eCFR-63)

Research that does not meet the criteria of "fundamental research" cannot involve foreign persons without export licenses; however, research activities that are considered fundamental typically can involve foreign persons, even when they involve the design and construction of defense articles, as the US State Department has deemed such research activities to fall outside of the purview of training activities that would constitute the illegal export of a "defense service."[[64]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Goodkin-64) The need to make this distinction has led many U.S. research universities to adopt ITAR policies and compliance programs. These measures can vary widely; for example, [MIT](https://en.wikipedia.org/wiki/MIT) states that "the intent of the ITAR is that research conducted on campus, without restrictions on publication or participation, is fundamental research from inception to publication as long as the intent is to publish the results,"[[65]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-MIT_OSP-65) while [Stanford University](https://en.wikipedia.org/wiki/Stanford_University) maintains a more nuanced and restrictive approach to research involving defense articles.[[66]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Stanford_DoResearch-66)

University interpretation and up-to-date understanding of export control regulations and willingness to seek opinions from the U.S. State Department affect the research that can be conducted on their campuses; for example, the University of Michigan successfully obtained an opinion from the Department of State stating that satellite development work on an (at the time) ITAR-controlled satellite being conducted by a student group containing both U.S. and non-U.S. citizens was considered fundamental research and was allowed to proceed.[[64]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Goodkin-64) In contrast, as of March 2016, Stanford's Export Control Officer maintains that all satellite systems are controlled defense articles under the ITAR (despite their [reclassification](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#satellite_reclassification) under the EAR in 2014) and, based on NASA criteria for *automatic* designation of a research project as fundamental research,[[67]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-NASA_NPR-67) does not consider projects above [TRL](https://en.wikipedia.org/wiki/Technology_readiness_level) 4 to be fundamental research, limiting the activities of laboratories and project-based groups on campus.[[68]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Eisner-68) This and similar policies are particularly damaging to international students studying aerospace engineering or related fields at U.S. universities, as opportunities to gain practical experience in their studies through internships are, due to licensing requirements, typically not offered to them at U.S. aerospace companies, and on-campus projects, when allowed, offer an alternate route for developing skills like those obtained through internships and co-op programs.

**Effects on the U.S. space industry**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=14)]

The Department of State insists that ITAR has limited effect and provides a security benefit to the nation that outweighs any impact that these sectors must bear. Every year, the Department of State can cite multiple arrests of ITAR violators by U.S. Immigration and Customs Enforcement agents and the [FBI](https://en.wikipedia.org/wiki/FBI).[[69]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-69) It is apparent that companies and institutions within the affected areas are somewhat stifled by ITAR regulations, in addition to the trade the U.S. economy would receive, and the science technology that it would share, notwithstanding that its restrictions encourage U.S. allies (such as Australia and the UK) to procure defense equipment from other sources that may not be interoperable with U.S. equipment.[[70]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-70) Companies argue that ITAR is a significant trade barrier that acts as a substantial negative subsidy, weakening U.S. industries' ability to compete.[[71]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Weinberger-71) U.S. companies point to announcements in Europe by TAS ([Thales Alenia Space](https://en.wikipedia.org/wiki/Thales_Alenia_Space)) promoting their "ITAR-free" telecommunication satellites.[[61]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-sattoday08-61)[[72]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-72)[[73]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-73)[[74]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-74) In 2008, officials at the Department of State dismissed the burden on industry and educational institutions as minor compared to the contributions to national security provided by ITAR. They also view the announcements of "ITAR-free" items as anecdotal and not systemic.[[61]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-sattoday08-61)[[*needs update*](https://en.wikipedia.org/wiki/Wikipedia:Manual_of_Style/Dates_and_numbers#Chronological_items)]

There is evidence that ITAR considerations have been a factor in decisions by foreign governments to avoid U.S. products and decisions by U.S. companies to remove USML items from their products:

* In April 2006, the [Australian Government](https://en.wikipedia.org/wiki/Government_of_Australia) was reported to have chosen [EADS](https://en.wikipedia.org/wiki/EADS) [MRH-90](https://en.wikipedia.org/wiki/NHI_NH90) troop-lift helicopters in preference to U.S. [Sikorsky](https://en.wikipedia.org/wiki/Sikorsky_Aircraft) models because "the European bid offered the ADF better access to crucial computer source code than the Sikorsky bid".[[75]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Barker-75)
* ITAR controls, as well as separate policy concerns, have hampered international cooperation in development of the [F-35 Lightning II](https://en.wikipedia.org/wiki/F-35_Lightning_II), also known as the [Joint Strike Fighter](https://en.wikipedia.org/wiki/Joint_Strike_Fighter) (JSF). Both the UK and the Australian governments demanded a guarantee that the U.S. will fully disclose technology needed for the JSF project before they would commit to further involvement in the project.[[76]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-Blenkin-76)[[77]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-77)[[78]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-78)
* Concerns over connections between the [Boeing 787](https://en.wikipedia.org/wiki/Boeing_787) and the [B-2 Spirit](https://en.wikipedia.org/wiki/B-2_Spirit) stealth bomber prompted [Boeing](https://en.wikipedia.org/wiki/Boeing) to take elaborate steps cleansing the commercial jet of any military technology. The issue arose when Boeing engineers, fearing indictment and penalties, refused to sign forms declaring that the 787 was "ITAR-free." As a result, Boeing conducted extensive research on the source of technology implemented on the 787. They removed all military technology and either found a commercial source for the same technology or replaced it with technology derived from a commercial source.[[79]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-79)
* For the F-X2 program, the Brazilian government have chosen the French [Dassault](https://en.wikipedia.org/wiki/Dassault_Aviation) [Rafale](https://en.wikipedia.org/wiki/Dassault_Rafale) over the Boeing [F/A-18E/F Super Hornet](https://en.wikipedia.org/wiki/Boeing_F/A-18E/F_Super_Hornet) due to concerns over technology transfer barriers and ITAR regulations, regardless that the [Brazilian Air Force](https://en.wikipedia.org/wiki/Brazilian_Air_Force) and the majority of their pilots preferred the Super Hornet over other bidders.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] Nelson Jobim, Defense minister of Brazil, said: "the U.S. government could give no upfront guarantee and Brazil had seen a series of U.S. technology embargoes." The lucrative contract, which will be signed after the 2010 Brazilian elections[[*needs update*](https://en.wikipedia.org/wiki/Wikipedia:Manual_of_Style/Dates_and_numbers#Chronological_items)], is for 36 aircraft and will be extended to over 100 units in the next decade.[[80]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-80)[[81]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-81)

**Registration fees**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=15)]

The U.S. Department of State charges back fees to manufacturers who have failed to register previously.[[82]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-faqs-82) Smaller exporters who may not have been aware of the requirement to register can potentially be charged crippling back fees when they first register.[[83]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-minutes-83) Allegations have been put to the U.S. Department of State-industry advisory group, the Defense Trade Advisory Group, that charging back fees discourages some manufacturers from registration.[[83]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-minutes-83)

**Restrictions on foreign products**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=16)]

Restrictions on Retransfer of USML items can also cause difficulties where those items have been incorporated into a product manufactured by a foreign person. If the foreign person wants to Retransfer the product to another foreign person, it must obtain authorization from the U.S. Government before the Retransfer can take place.

It is open to the U.S. Government to refuse to authorize Retransfer of a foreign product that includes USML items:

* in 2006, the U.S. Government refused to authorize the sale of [C-295](https://en.wikipedia.org/wiki/C-295) transport and maritime patrol aircraft manufactured by the Spanish aircraft manufacturer, [EADS-CASA](https://en.wikipedia.org/wiki/EADS-CASA), to Venezuela because the aircraft included US-origin avionics and engine components controlled under the USML. As a consequence, EADS-CASA was forced to cancel a €500 million contract with Venezuela;[[84]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-84)[[85]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-85) and
* in 2006, [Embraer](https://en.wikipedia.org/wiki/Embraer) of Brazil was also prevented from selling [Super Tucano](https://en.wikipedia.org/wiki/Super_Tucano) aircraft to Venezuela by the U.S.[[86]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-86)

As a consequence of the blocking of these sales, Venezuela has subsequently purchased aircraft and other military hardware from Russia and Belarus.[[87]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-87)

* In 2010 the [*Halifax*-class](https://en.wikipedia.org/wiki/Halifax-class_frigate) frigate will be using as much non-American equipment as possible, including technology from Canada, Sweden, Germany, the Netherlands and Israel. The International Traffic in Arms Regulations have also been blamed for the delay of the [CH-148 Cyclone](https://en.wikipedia.org/wiki/CH-148_Cyclone) which is currently two years behind the original schedule.[[88]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-88)
* In 2010 the [Sikorsky CH-148 Cyclone](https://en.wikipedia.org/wiki/Sikorsky_CH-148_Cyclone) helicopter was faced with delays and restrictions. The first 19 of the 28 CH-148 Cyclones will be delivered in an interim standard which does not meet the original contract requirements.[[89]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-89)

**Restrictions on Dual and Third Country Nationals**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=17)]

The restrictions on access to USML items by Dual and Third Country National employees of a foreign person can cause significant difficulties because the current accepted definitions of Dual and Third Country Nationals do not reflect the definition of "US persons". The Department of State defines Dual and Third Country Nationality as follows:

* Third Country National: An individual holding nationality from a country or countries other than the country of the foreign signatory to the agreement; and
* Dual National: Holds nationality from the country of a foreign signatory and one or more additional foreign countries.[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27):17

Although "nationality" is not defined under ITAR, it is accepted that the U.S. Government will take country of origin[[27]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-SAG-27) and continued ties or allegiance to a country into account when determining Dual or Third Country Nationality.[[90]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-90)[[91]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-91)

This means that a person who was born in the UK but is a U.S. permanent resident working in the U.S. for a U.S. company will be considered a U.S. person only (under the definition of "US person"). If, however, the same person emigrated to Canada, obtained [Canadian citizenship](https://en.wikipedia.org/wiki/Canadian_citizenship) and commenced employment with a Canadian company, she would be treated as a Canadian-UK Dual National for the purposes of any U.S. export authorization to which her employer was a party. If she did not obtain Canadian citizenship but instead became a temporary or permanent Canadian resident, she would be treated as a UK Third Country National for the purposes of such U.S. export authorization.[[28]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-defence.gov.au-28)

It is also possible for a person who was born in one country to become a Dual National for the purposes of ITAR without necessarily leaving his country of origin, simply by obtaining a foreign passport (thereby "holding nationality" from another country). This is frequently the case where the individual's parent/s were born in a country that grants citizenship to children of its citizens, regardless of where the children were born, for example, a child born in Canada to parents who were born in the UK is able to obtain a UK passport (see [British nationality law](https://en.wikipedia.org/wiki/British_nationality_law)). Once he has done so, he becomes a Canadian-UK Dual National for the purposes of ITAR.

Restrictions on access to USML items by Dual and Third Country National employees of foreign persons essentially forces foreign persons to discriminate against their employees who do not meet the nationality criteria under an export authorization. Such discrimination may be illegal in some countries under [anti-discrimination law](https://en.wikipedia.org/wiki/Anti-discrimination_law) (such as in Canada[[92]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-92)[[93]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-93) and Australia).[[33]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-abc.net.au-33)

In addition, the prohibition on access by Dual and Third Country Nationals from countries proscribed under ITAR 126.1 can cause problems for countries with large immigrant populations from those countries (such as Canada and Australia, which both have large [Overseas Chinese](https://en.wikipedia.org/wiki/Overseas_Chinese) and [Overseas Vietnamese](https://en.wikipedia.org/wiki/Overseas_Vietnamese) immigrant populations: see [immigration to Canada](https://en.wikipedia.org/wiki/Immigration_to_Canada) and [immigration to Australia](https://en.wikipedia.org/wiki/Immigration_to_Australia)).[[33]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-abc.net.au-33)

The U.S. Government actively enforces restrictions on access to USML items by Dual and Third Country Nationals:

* [General Dynamics Land Systems](https://en.wikipedia.org/wiki/General_Dynamics_Land_Systems) was fined US$20m in 2004 for breaches of the AECA by its predecessor, [GM Defense](https://en.wikipedia.org/wiki/GM_Defense), that included access to USML items by unauthorized Dual Nationals. The unauthorized access had included direct access to USML items and access to international computer systems on which USML items were stored by Dual Nationals from countries including Syria and the PRC.[[94]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-gmgd-94)

**ITAR and information technology**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=18)]

The ease with which USML items can be exported and retransferred using computer networks and removable media significantly increases the risk of unauthorized retransfer of USML items. As discussed above, carrying a laptop computer which contains USML items overseas is considered a retransfer of those items. Likewise, access to USML items on corporate systems, such as intranets, by foreign persons overseas or in the U.S., is considered a Retransfer of the items.[[94]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-gmgd-94) Foreign employees working in the US cannot have access to the same network where ITAR data may be stored, nor may they have access to rooms or facilities where ITAR work is being done.[[95]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-:0-95)

It is important to note that, in both cases, theoretical access to the USML items overseas or by foreign persons is sufficient to constitute a breach of ITAR.[[94]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-gmgd-94) Files on a laptop carried overseas do not need to be opened overseas, and foreign persons do not need to have actual access to USML items on computer networks for a breach to occur.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Theoretical access to USML items by foreign persons (including dual and third country nationals) can create difficulties for the engagement of IT professionals from overseas as network administrators or the use of overseas companies to support IT systems.[[96]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-96) This also creates significant challenges for manufacturers of ITAR-related items with respect to hiring practices. Avoiding discrimination while screening applicants for their ability to access ITAR materials can often be an HR nightmare.[[95]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-:0-95)

**Exemptions and treaties**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=19)]

Several countries have sought ITAR exemptions or treaties with the U.S. Government in an effort to minimize the impact of ITAR, with varying degrees of success. The U.S. Government remains reluctant to consider broad exemptions from ITAR because of continuing concerns regarding the adverse effect unauthorized release of USML items can have on U.S. national security.[[97]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-97)

[](https://en.wikipedia.org/wiki/File:Ac.hhyde.jpg)

Congressman [Henry Hyde](https://en.wikipedia.org/wiki/Henry_Hyde) repeatedly blocked an ITAR waiver for the UK.

Canada is the recipient of an ITAR exemption related to the 1963 Defense Development Sharing Arrangement with the U.S. Government.[[98]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-98)[[99]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-99)[[100]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-100)[[101]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-101)

Attempts by the UK Government to obtain a similar exemption were also stymied. The UK Government sought an exemption in the context of the JSF project. The Clinton administration promised the United Kingdom's [Ministry of Defence](https://en.wikipedia.org/wiki/Ministry_of_Defence_(United_Kingdom)) that an ITAR waiver would be given, allowing greater technology transfer associated with the project.[[102]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-102) Yet, despite the backing of the Bush administration, the waiver was repeatedly blocked by the late U.S. Congressman [Henry Hyde](https://en.wikipedia.org/wiki/Henry_Hyde) because of his security concerns about potential technology transfer to third countries.[[103]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-103) With his departure, ITAR-related impacts regarding the F-35 / JSF program remain in flux. These difficulties caused the UK to threaten that it would abandon the JSF project and consider alternative aircraft.[[104]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-104)

The U.S. Government signed bilateral defense trade cooperation [treaties](https://en.wikipedia.org/wiki/Treaties) with the UK and Australian governments in June[[105]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-105)[[106]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-106) and September 2007[[107]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-107)[[108]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-108) respectively. The treaties are designed to allow the exchange of technical data, defense articles and defense services (including USML items) without the need for export authorizations such as TAAs and MLAs, subject to restrictions on the type and classification of the technology in question and its intended end-use.[[109]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-109)[[110]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-110) In return, the UK and Australian governments will be required to take steps to improve their export control laws (such as the Australian [Customs Act](https://en.wikipedia.org/w/index.php?title=Customs_Act&action=edit&redlink=1)).[[111]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-111) As of September 2008, the U.S. [Senate Foreign Relations Committee](https://en.wikipedia.org/wiki/Senate_Foreign_Relations_Committee) had deferred consideration of the treaties on the grounds that it had not had time to properly evaluate proposed amendments to ITAR required in order to implement the treaties.[[112]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-112)[[113]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-113)

There have been exemptions for scientific research: notably certain specialized components used in the Large Hadron Collider are "dual use" but as the US contributes both research grant money and personnel it is generally believed[[*by whom?*](https://en.wikipedia.org/wiki/Wikipedia:Manual_of_Style/Words_to_watch#Unsupported_attributions)] that a reciprocal arrangement exists.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**Satellite components**[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=20)]

Before 1992, satellite components were classified as munitions, and ITAR export compliance was controlled by the State Department.[[114]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-zenio2006-114) After the [Space Shuttle Challenger disaster](https://en.wikipedia.org/wiki/Space_Shuttle_Challenger_disaster) resulted in a growing backlog of commercial satellite launches, ITAR kept the Soviet Union out of the market. In September 1988, U.S. President [Ronald Reagan](https://en.wikipedia.org/wiki/Ronald_Reagan) agreed to allow U.S satellites to be launched on Chinese rockets.[[115]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-115) Communications satellites were gradually transferred from the State Department to the Commerce Department in 1992–1996, falling under the [Export Administration Regulations](https://en.wikipedia.org/wiki/Export_Administration_Regulations).[[114]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-zenio2006-114)[[116]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-zinger2014-116)

After the failed launches of [Apstar 2](https://en.wikipedia.org/wiki/Apstar_2) (1995) and [Intelsat 708](https://en.wikipedia.org/wiki/Intelsat_708) (1996), the [satellite insurance](https://en.wikipedia.org/wiki/Satellite_insurance) companies required the satellite manufacturers to work with China to investigate the failures. The Commerce Department determined that the "export" of information as part of the failure analysis complied with the export license.[[114]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-zenio2006-114) However, the Justice Department maintained that a separate export license was required in addition to the original launch license. In 1998, Congress reclassified satellite technology as a munition and returned it to the control of the State Department under ITAR.[[116]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-zinger2014-116) [Space Systems/Loral](https://en.wikipedia.org/wiki/Space_Systems/Loral) paid a $20 million fine in 2002, and Boeing paid a $32 million fine in 2003 on behalf of its Hughes subsidiary. The [ChinaSat 8](https://en.wikipedia.org/wiki/Chinasat#ChinaSat_8) satellite, which had been scheduled for launch in April 1999 on a [Long March 3B](https://en.wikipedia.org/wiki/Long_March_3B) rocket,[[117]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-117) was placed in storage for a decade and finally launched on an [Ariane 5](https://en.wikipedia.org/wiki/Ariane_5) rocket in 2008.[[114]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-zenio2006-114)

China used the results of the insurance investigation to improve the reliability of its [Long March rockets](https://en.wikipedia.org/wiki/Long_March_(rocket_family)), which would not experience another mission failure until 2011.[[118]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-118) ITAR has been blamed for "destroy[ing] an industry," reducing the market share of U.S. satellite makers by almost 25% from 1997 to 2007.[[116]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-zinger2014-116) The European company [Thales Alenia Space](https://en.wikipedia.org/wiki/Thales_Alenia_Space) developed a line of ITAR-free satellites that used no restricted U.S. components, allowing them to be launched on Chinese rockets between 2005 and 2012.[[119]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-119) However, the U.S. Department of State did not accept the ITAR-free status of these satellites and fined the US company Aeroflex $8 million for selling ITAR components. Thales Alenia was forced to discontinue its ITAR-free satellite line in 2013.[[120]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-120)

In May 2014, the United States Department of State reclassified satellites and several related components so they will no longer be treated as munitions whose export is controlled by ITAR, but will be covered instead under the [Export Administration Regulations](https://en.wikipedia.org/wiki/Export_Administration_Regulations).[[121]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-121) These new classifications took effect in November 2014, six months after the announcement of the reclassification.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] Restrictions were loosened on 36 countries, strict controls remained on another 150 countries, and exports remained prohibited to 20 countries. An official at the [Bureau of Industry and Security](https://en.wikipedia.org/wiki/Bureau_of_Industry_and_Security) emphasized that "no U.S.-origin content, regardless of significance, regardless of whether it’s incorporated into a foreign-made item, can go to China."[[122]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-selding2016-122) Thales Alenia had long complained that "every satellite nut and bolt" was being classified as ITAR-restricted, and the [European Space Agency](https://en.wikipedia.org/wiki/European_Space_Agency) accused the United States of having no real interest in protecting U.S. satellite technology.[[123]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-123)

ITAR remains a major concern in the European aerospace industry as of 2016. The [European Space Agency](https://en.wikipedia.org/wiki/European_Space_Agency) and the [Japanese Aerospace Exploration Agency](https://en.wikipedia.org/wiki/JAXA) have supplied components that were launched on Chinese rockets. European manufacturers of satellite components report that ITAR-free status is the first question they are asked by potential customers. Even U.S. companies have expressed interest in ITAR-free technology.[[122]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-selding2016-122) The Chinese space industry has been able to sell in the global market by [bundling](https://en.wikipedia.org/wiki/Product_bundling) Chinese satellites with Chinese rockets, avoiding ITAR.[[124]](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations#cite_note-124)

See also[[edit](https://en.wikipedia.org/w/index.php?title=International_Traffic_in_Arms_Regulations&action=edit&section=21)]

* [Arms Export Control Act](https://en.wikipedia.org/wiki/Arms_Export_Control_Act)
* [CoCom](https://en.wikipedia.org/wiki/CoCom)
* [Defense Security Cooperation Agency](https://en.wikipedia.org/wiki/Defense_Security_Cooperation_Agency)
* [Under Secretary for Arms Control and International Security](https://en.wikipedia.org/wiki/Under_Secretary_for_Arms_Control_and_International_Security)
* [Export Control Classification Number](https://en.wikipedia.org/wiki/Export_Control_Classification_Number)

About NERC-CIP Industries: Utilities and Energy

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long‐term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC’s area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 400 million people.

The History of the North American Electric Reliability Corporation(NERC)

<https://www.nerc.com/AboutNERC/Resource%20Documents/NERCHistoryBook.pdf>

Board of Trustees

<https://www.nerc.com/gov/bot/Pages/default.aspx>

The **NERC CIP** (North American Electric Reliability Corporation critical infrastructure protection) plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [CIP-002-5.1a.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf) | [CIP-002-5.1a](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf) | [Cyber Security — BES Cyber System Categorization](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber%20Security%20%E2%80%94%20BES%20Cyber%20System%20Categorization) | [Related Information](http://www.nerc.com/pa/Stand/Pages/CIP0025.1aRI.aspx) | Subject to Enforcement |
| [CIP-003-8.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-8.pdf) | [CIP-003-8](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-8.pdf) | [Cyber Security — Security Management Controls](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-003-8&title=Cyber%20Security%20%E2%80%94%20Security%20Management%20Controls) |  | Subject to Enforcement |
| [CIP-004-6.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-004-6.pdf) | [CIP-004-6](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-004-6.pdf) | [Cyber Security - Personnel & Training](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-004-6&title=Cyber%20Security%20-%20Personnel%20&%20Training) | [Related Information](https://www.nerc.com/pa/Stand/Pages/CIP0046RI.aspx) | Subject to Enforcement |
| [CIP-005-5.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf) | [CIP-005-5](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf) | [Cyber Security - Electronic Security Perimeter(s)](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-005-5&title=Cyber%20Security%20-%20Electronic%20Security%20Perimeter(s)) | [Related Information](https://www.nerc.com/pa/Stand/Pages/CIP0055RI.aspx) | Subject to Enforcement |
| [CIP-006-6.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-006-6.pdf) | [CIP-006-6](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-006-6.pdf) | [Cyber Security - Physical Security of BES Cyber Systems](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-006-6&title=Cyber%20Security%20-%20Physical%20Security%20of%20BES%20Cyber%20Systems) | [Related Information](https://www.nerc.com/pa/Stand/Pages/CIP0066RI.aspx) | Subject to Enforcement |
| [CIP-007-6.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-6.pdf) | [CIP-007-6](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-6.pdf) | [Cyber Security - System Security Management](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-007-6&title=Cyber%20Security%20-%20System%20Security%20Management) | [Related Information](https://www.nerc.com/pa/Stand/Pages/CIP0076RI.aspx) | Subject to Enforcement |
| [CIP-008-5.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-5.pdf) | [CIP-008-5](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-5.pdf) | [Cyber Security - Incident Reporting and Response Planning](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-008-5&title=Cyber%20Security%20-%20Incident%20Reporting%20and%20Response%20Planning) | [Related Information](https://www.nerc.com/pa/Stand/Pages/CIP0085RI.aspx) | Subject to Enforcement |
| [CIP-009-6.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-009-6.pdf) | [CIP-009-6](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-009-6.pdf) | [Cyber Security - Recovery Plans for BES Cyber Systems](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-009-6&title=Cyber%20Security%20-%20Recovery%20Plans%20for%20BES%20Cyber%20Systems) | [Related Information](https://www.nerc.com/pa/Stand/Pages/CIP0096RI.aspx) | Subject to Enforcement |
| [CIP-010-2.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-2.pdf) | [CIP-010-2](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-2.pdf) | [Cyber Security - Configuration Change Management and Vulnerability Assessments](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-010-2&title=Cyber%20Security%20-%20Configuration%20Change%20Management%20and%20Vulnerability%20Assessments) | [Related Information](https://www.nerc.com/pa/Stand/Pages/CIP-0102RI.aspx) | Subject to Enforcement |
| [CIP-011-2.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-011-2.pdf) | [CIP-011-2](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-011-2.pdf) | [Cyber Security - Information Protection](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-011-2&title=Cyber%20Security%20-%20Information%20Protection) | [Related Information](https://www.nerc.com/pa/Stand/Pages/CIP0112RI.aspx) | Subject to Enforcement |
| [CIP-014-2.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf) | [CIP-014-2](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf) | [Physical Security](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=Physical%20Security) | [Related Information](http://www.nerc.com/pa/Stand/Pages/CIP014-2RI.aspx) | Subject to Enforcement |

About HIPAA HITECH Industry Medical and Financial

<https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act>

The **Health Insurance Portability and Accountability Act of 1996** (**HIPAA** or the [Kennedy](https://en.wikipedia.org/wiki/Ted_Kennedy)–[Kassebaum](https://en.wikipedia.org/wiki/Nancy_Kassebaum) Act[[1]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-Atchinson/Fox-1)[[2]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-2)) was enacted by the [104th United States Congress](https://en.wikipedia.org/wiki/104th_United_States_Congress) and signed by President [Bill Clinton](https://en.wikipedia.org/wiki/Bill_Clinton) in 1996. It was created primarily to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage.[[3]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-3)

The act consists of five titles. Title I of HIPAA protects [health insurance](https://en.wikipedia.org/wiki/Health_insurance_in_the_United_States) coverage for workers and their families when they change or lose their jobs.[[4]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-4) Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for [electronic health care](https://en.wikipedia.org/wiki/Electronic_health_record) transactions and national identifiers for providers, health insurance plans, and employers.[[5]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-5) Title III sets guidelines for pre-tax medical spending accounts, Title IV sets guidelines for group health plans, and Title V governs company-owned life insurance policies.



**Contents**

* [1Titles](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Titles)
  + [1.1Title I: Health Care Access, Portability, and Renewability](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Title_I:_Health_Care_Access,_Portability,_and_Renewability)
  + [1.2Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Title_II:_Preventing_Health_Care_Fraud_and_Abuse;_Administrative_Simplification;_Medical_Liability_Reform)
    - [1.2.1Privacy Rule](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Privacy_Rule)
      * [1.2.1.12013 Final Omnibus Rule Update](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#2013_Final_Omnibus_Rule_Update)
        + [1.2.1.1.1HITECH Act: Privacy Requirements](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#HITECH_Act:_Privacy_Requirements)
      * [1.2.1.2Right to access your PHI](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Right_to_access_your_PHI)
      * [1.2.1.3Disclosure to relatives](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Disclosure_to_relatives)
    - [1.2.2Transactions and Code Sets Rule](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Transactions_and_Code_Sets_Rule)
      * [1.2.2.1Brief 5010 Transactions and Code Sets Rules Update Summary](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Brief_5010_Transactions_and_Code_Sets_Rules_Update_Summary)
    - [1.2.3Security Rule](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Security_Rule)
    - [1.2.4Unique Identifiers Rule (National Provider Identifier)](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Unique_Identifiers_Rule_(National_Provider_Identifier))
    - [1.2.5Enforcement Rule](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Enforcement_Rule)
  + [1.3Title III: Tax-related health provisions governing medical savings accounts](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Title_III:_Tax-related_health_provisions_governing_medical_savings_accounts)
  + [1.4Title IV: Application and enforcement of group health insurance requirements](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Title_IV:_Application_and_enforcement_of_group_health_insurance_requirements)
  + [1.5Title V: Revenue offset governing tax deductions for employers](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Title_V:_Revenue_offset_governing_tax_deductions_for_employers)
* [2Effects on research and clinical care](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Effects_on_research_and_clinical_care)
  + [2.1Effects on research](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Effects_on_research)
  + [2.2Effects on clinical care](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Effects_on_clinical_care)
  + [2.3Costs of implementation](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Costs_of_implementation)
  + [2.4Education and training](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Education_and_training)
* [3HIPAA acronym](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#HIPAA_acronym)
* [4Violations](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Violations)
* [5Legislative information](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Legislative_information)
* [6References](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#References)
* [7External links](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#External_links)

**Title I: Health Care Access, Portability, and Renewability**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=2)]

Title I of HIPAA regulates the availability and breadth of group health plans and certain individual health insurance policies. It amended the Employee Retirement Income Security Act, the Public Health Service Act, and the Internal Revenue Code.

Title I requires the coverage of and also limits restrictions that a group health plan can place on benefits for preexisting conditions. Group health plans may refuse to provide benefits in relation to preexisting conditions for either 12 months following enrollment in the plan or 18 months in the case of late enrollment.[[6]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-6) Title I allows individuals to reduce the exclusion period by the amount of time that they have had "creditable coverage" before enrolling in the plan and after any "significant breaks" in coverage.[[7]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-7) "Creditable coverage" is defined quite broadly and includes nearly all group and individual health plans, Medicare, and Medicaid.[[8]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-8) A "significant break" in coverage is defined as any 63-day period without any creditable coverage.[[9]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-9) Along with an exception, allowing employers to tie premiums or co-payments to tobacco use, or body mass index.

Title I[[10]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-10) also requires insurers to issue policies without exclusion to those leaving group health plans with creditable coverage (see above) exceeding 18 months, and[[11]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-11) renew individual policies for as long as they are offered or provide alternatives to discontinued plans for as long as the insurer stays in the market without exclusion regardless of health condition.

Some health care plans are exempted from Title I requirements, such as long-term health plans and limited-scope plans like dental or vision plans offered separately from the general health plan. However, if such benefits are part of the general health plan, then HIPAA still applies to such benefits. For example, if the new plan offers dental benefits, then it must count creditable continuous coverage under the old health plan towards any of its exclusion periods for dental benefits.

An alternate method of calculating creditable continuous coverage is available to the health plan under Title I. That is, 5 categories of health coverage can be considered separately, including dental and vision coverage. Anything not under those 5 categories must use the general calculation (e.g., the beneficiary may be counted with 18 months of general coverage, but only 6 months of dental coverage, because the beneficiary did not have a general health plan that covered dental until 6 months prior to the application date). Since limited-coverage plans are exempt from HIPAA requirements, the odd case exists in which the applicant to a general group health plan cannot obtain certificates of creditable continuous coverage for independent limited-scope plans, such as dental to apply towards exclusion periods of the new plan that does include those coverages.

Hidden exclusion periods are not valid under Title I (e.g., "The accident, to be covered, must have occurred while the beneficiary was covered under this exact same health insurance contract"). Such clauses must not be acted upon by the health plan. Also, they must be re-written so they can comply with HIPAA.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=3)]

|  |  |
| --- | --- |
|  | This section **needs additional citations for**[**verification**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability). Please help [improve this article](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit) by [adding citations to reliable sources](https://en.wikipedia.org/wiki/Help:Introduction_to_referencing_with_Wiki_Markup/1). Unsourced material may be challenged and removed. *Find sources:* ["Health Insurance Portability and Accountability Act"](https://www.google.com/search?as_eq=wikipedia&q=%22Health+Insurance+Portability+and+Accountability+Act%22) – [news](https://www.google.com/search?tbm=nws&q=%22Health+Insurance+Portability+and+Accountability+Act%22+-wikipedia) **·** [newspapers](https://www.google.com/search?&q=%22Health+Insurance+Portability+and+Accountability+Act%22+site:news.google.com/newspapers&source=newspapers) **·** [books](https://www.google.com/search?tbs=bks:1&q=%22Health+Insurance+Portability+and+Accountability+Act%22+-wikipedia) **·** [scholar](https://scholar.google.com/scholar?q=%22Health+Insurance+Portability+and+Accountability+Act%22) **·** [JSTOR](https://www.jstor.org/action/doBasicSearch?Query=%22Health+Insurance+Portability+and+Accountability+Act%22&acc=on&wc=on) *(April 2010) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

Title II of HIPAA establishes policies and procedures for maintaining the privacy and the security of individually identifiable health information, outlines numerous offenses relating to health care, and establishes civil and criminal penalties for violations. It also creates several programs to control fraud and abuse within the health-care system.[[12]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-12)[[13]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-13)[[14]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-14)[[15]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-auto-15) However, the most significant provisions of Title II are its Administrative Simplification rules. Title II requires the [Department of Health and Human Services](https://en.wikipedia.org/wiki/United_States_Department_of_Health_and_Human_Services) (HHS) to increase the efficiency of the health-care system by creating standards for the use and dissemination of health-care information.[[15]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-auto-15)

These rules apply to "covered entities", as defined by HIPAA and the HHS. Covered entities include health plans, health care clearinghouses (such as billing services and community health information systems), and health care providers that transmit health care data in a way regulated by HIPAA.[[16]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-CodeFedReg|45|160|103-16)[[17]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-17)

Per the requirements of Title II, the HHS has promulgated five rules regarding Administrative Simplification: the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, the Unique Identifiers Rule, and the Enforcement Rule.

**Privacy Rule**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=4)]

The HIPAA Privacy Rule is composed of national regulations for the use and disclosure of Protected Health Information (PHI) in healthcare treatment, payment and operations by covered entities.

The effective compliance date of the Privacy Rule was April 14, 2003, with a one-year extension for certain "small plans". The HIPAA Privacy Rule regulates the use and disclosure of [protected health information](https://en.wikipedia.org/wiki/Protected_health_information) (PHI) held by "covered entities" (generally, health care clearinghouses, employer-sponsored health plans, health insurers, and medical service providers that engage in certain transactions).[[18]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-18) By regulation, the HHS extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "business associates".[[19]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-19) PHI is any information that is held by a covered entity regarding health status, provision of health care, or health care payment that can be linked to any individual.[[16]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-CodeFedReg|45|160|103-16) This is interpreted rather broadly and includes any part of an individual's [medical record](https://en.wikipedia.org/wiki/Medical_record) or payment history. Covered entities must disclose PHI to the individual within 30 days upon request.[[20]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-20) Also, they must disclose PHI when required to do so by law such as reporting suspected [child abuse](https://en.wikipedia.org/wiki/Child_abuse) to state child welfare agencies.[[21]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-21)

Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; or to identify or locate a suspect, a fugitive, a material witness, or a missing person.[[22]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-22)

A covered entity may disclose PHI to certain parties to facilitate treatment, payment, or health care operations without a patient's express written authorization.[[23]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-23) Any other disclosures of PHI require the covered entity to obtain written authorization from the individual for the disclosure.[[24]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-24) In any case, when a covered entity discloses any PHI, it must make a reasonable effort to disclose only the minimum necessary information required to achieve its purpose.[[25]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-25)

The Privacy Rule gives individuals the right to request a covered entity to correct any inaccurate PHI.[[26]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-26) Also, it requires covered entities to take some reasonable steps on ensuring the confidentiality of communications with individuals.[[27]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-27) For example, an individual can ask to be called at their work number instead of home or cell phone numbers.

The Privacy Rule requires covered entities to notify individuals of uses of their PHI.[[28]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-28) Covered entities must also keep track of disclosures of PHI and document privacy policies and procedures.[[29]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-29) They must appoint a Privacy Official and a contact person[[30]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-30) responsible for receiving complaints and train all members of their workforce in procedures regarding PHI.[[31]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-31)

An individual who believes that the Privacy Rule is not being upheld can file a complaint with the Department of Health and Human Services Office for Civil Rights (OCR).[[32]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-32)[[33]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-33) However, according to the *Wall Street Journal*, the OCR has a long backlog and ignores most complaints. "Complaints of privacy violations have been piling up at the Department of Health and Human Services. Between April of 2003 and November 2006, the agency fielded 23,886 complaints related to medical-privacy rules, but it has not yet taken any enforcement actions against hospitals, doctors, insurers or anyone else for rule violations. A spokesman for the agency says it has closed three-quarters of the complaints, typically because it found no violation or after it provided informal guidance to the parties involved."[[34]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-34) However, in July 2011, UCLA agreed to pay $865,500 in a settlement regarding potential HIPAA violations. An HHS Office for Civil Rights investigation showed that from 2005 to 2008, unauthorized employees repeatedly and without legitimate cause looked at the electronic protected health information of numerous UCLAHS patients.[[35]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-35)

**2013 Final Omnibus Rule Update**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=5)]

In January 2013, HIPAA was updated via the Final Omnibus Rule.[[36]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-36) The updates included changes to the Security Rule and Breach Notification portions of the HITECH Act. The most significant changes related to the expansion of requirements to include business associates, where only covered entities had originally been held to uphold these sections of the law.[[37]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-37)

In addition, the definition of "significant harm" to an individual in the analysis of a breach was updated to provide more scrutiny to covered entities with the intent of disclosing breaches that previously were unreported. Previously, an organization needed proof that harm had occurred whereas now organizations must prove that harm had not occurred.

Protection of PHI was changed from indefinite to 50 years after death. More severe penalties for violation of PHI privacy requirements were also approved.[[38]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-38)

The HIPAA Privacy rule may be waived during natural disaster. This was the case with Hurricane Harvey in 2017.[[39]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-39)

**HITECH Act: Privacy Requirements**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=6)]

See the [Privacy section](https://en.wikipedia.org/wiki/Health_Information_Technology_for_Economic_and_Clinical_Health_Act#Subtitle_D_%E2%80%93_Privacy) of the [Health Information Technology for Economic and Clinical Health Act](https://en.wikipedia.org/wiki/Health_Information_Technology_for_Economic_and_Clinical_Health_Act) ([HITECH Act](https://en.wikipedia.org/wiki/HITECH_Act)).

**Right to access your PHI**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=7)]

The Privacy Rule requires medical providers to give individuals access to their PHI.[[40]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-40) After an individual requests information in writing (typically using the provider's form for this purpose), a provider has up to 30 days to provide a copy of the information to the individual. An individual may request the information in electronic form or hard-copy, and the provider is obligated to attempt to conform to the requested format. For providers using an electronic health record ([EHR](https://en.wikipedia.org/wiki/Electronic_health_record)) system that is certified using CEHRT (Certified Electronic Health Record Technology) criteria, individuals must be allowed to obtain the PHI in electronic form. Providers are encouraged to provide the information expediently, especially in the case of electronic record requests.

Individuals have the right to access all health-related information, including health condition, treatment plan, notes, images, lab results, and billing information. Explicitly excluded are the private psychotherapy notes of a provider, and information gathered by a provider to defend against a lawsuit.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Providers can charge a reasonable amount that relates to their cost of providing the copy, however, no charge is allowable when providing data electronically from a certified [EHR](https://en.wikipedia.org/wiki/Electronic_health_record) using the "view, download, and transfer" feature which is required for certification. When delivered to the individual in electronic form, the individual may authorize delivery using either encrypted or un-encrypted email, delivery using media (USB drive, CD, etc., which may involve a charge), direct messaging (a secure email technology in common use in the healthcare industry), or possibly other methods. When using un-encrypted email, the individual must understand and accept the risks to privacy using this technology (the information may be intercepted and examined by others). Regardless of delivery technology, a provider must continue to fully secure the PHI while in their system and can deny the delivery method if it poses additional risk to PHI while in their system.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

An individual may also request (in writing) that their PHI is delivered to a designated third party such as a family care provider.

An individual may also request (in writing) that the provider send PHI to a designated service used to collect or manage their records, such as a Personal Health Record application. For example, a patient can request in writing that her ob-gyn provider digitally transmit records of her latest pre-natal visit to a pregnancy self-care app that she has on her mobile phone.

**Disclosure to relatives**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=8)]

According to their interpretations of HIPAA, hospitals will not reveal information over the phone to relatives of admitted patients. This has in some instances impeded the location of missing persons. After the [Asiana Airlines Flight 214](https://en.wikipedia.org/wiki/Asiana_Airlines_Flight_214) San Francisco crash, some hospitals were reluctant to disclose the identities of passengers that they were treating, making it difficult for Asiana and the relatives to locate them.[[41]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-41) In one instance, a man in Washington state was unable to obtain information about his injured mother.[[42]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-42)

Janlori Goldman, director of the advocacy group Health Privacy Project, said that some hospitals are being "overcautious" and misapplying the law, the Times reports. Suburban Hospital in Bethesda, Md., has interpreted a federal regulation that requires hospitals to allow patients to opt out of being included in the hospital directory as meaning that patients want to be kept out of the directory unless they specifically say otherwise. As a result, if a patient is unconscious or otherwise unable to choose to be included in the directory, relatives and friends might not be able to find them, Goldman said.[[43]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-43)

**Transactions and Code Sets Rule**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=9)]

HIPAA was intended to make the health care system in the United States more efficient by standardizing health care transactions. HIPAA added a new Part C titled "Administrative Simplification" to Title XI of the Social Security Act.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] This is supposed to simplify healthcare transactions by requiring all health plans to engage in health care transactions in a standardized way.

The HIPAA/EDI provision was scheduled to take effect from October 16, 2003, with a one-year extension for certain "small plans". However, due to widespread confusion and difficulty in implementing the rule, CMS granted a one-year extension to all parties.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] On January 1, 2012 newer versions, [ASC X12](https://en.wikipedia.org/wiki/ASC_X12) 005010 and NCPDP D.0 become effective, replacing the previous ASC X12 004010 and NCPDP 5.1 mandate.[[44]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-44) The ASC X12 005010 version provides a mechanism allowing the use of [ICD-10-CM](https://en.wikipedia.org/wiki/ICD-10-CM) as well as other improvements.

After July 1, 2005 most medical providers that file electronically had to file their electronic claims using the HIPAA standards in order to be paid.[[45]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-45)

Under HIPAA, HIPAA-covered health plans are now required to use standardized HIPAA electronic transactions. See, 42 USC § 1320d-2 and 45 CFR Part 162. Information about this can be found in the final rule for HIPAA electronic transaction standards (74 Fed. Reg. 3296, published in the Federal Register on January 16, 2009), and on the CMS website.[[46]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-46)

Key [EDI](https://en.wikipedia.org/wiki/Electronic_data_interchange) (X12) transactions used for HIPAA compliance are:[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**EDI Health Care Claim Transaction set (837)** is used to submit health care claim billing information, encounter information, or both, except for retail pharmacy claims (see EDI Retail Pharmacy Claim Transaction). It can be sent from providers of health care services to payers, either directly or via intermediary billers and claims clearinghouses. It can also be used to transmit health care claims and billing payment information between payers with different payment responsibilities where coordination of benefits is required or between payers and regulatory agencies to monitor the rendering, billing, and/or payment of health care services within a specific health care/insurance industry segment.

For example, a state mental health agency may mandate all healthcare claims, Providers and health plans who trade professional (medical) health care claims electronically must use the 837 Health Care Claim: Professional standard to send in claims. As there are many different business applications for the Health Care claim, there can be slight derivations to cover off claims involving unique claims such as for institutions, professionals, chiropractors, and dentists etc.

**EDI Retail Pharmacy Claim Transaction (**[**NCPDP**](https://en.wikipedia.org/wiki/NCPDP)**Telecommunications Standard version 5.1)** is used to submit retail pharmacy claims to payers by health care professionals who dispense medications, either directly or via intermediary billers and claims clearinghouses. It can also be used to transmit claims for retail pharmacy services and billing payment information between payers with different payment responsibilities where coordination of benefits is required or between payers and regulatory agencies to monitor the rendering, billing, and/or payment of retail pharmacy services within the pharmacy health care/insurance industry segment.

**EDI Health Care Claim Payment/Advice Transaction Set (835)** can be used to make a payment, send an Explanation of Benefits (EOB), send an Explanation of Payments (EOP) [remittance advice](https://en.wikipedia.org/wiki/Remittance_advice), or make a payment and send an EOP remittance advice only from a health insurer to a health care provider either directly or via a financial institution.

[**EDI Benefit Enrollment and Maintenance Set (834)**](https://en.wikipedia.org/wiki/ANSI_834_Enrollment_Implementation_Format) can be used by employers, unions, government agencies, associations or insurance agencies to enroll members to a payer. The payer is a healthcare organization that pays claims, administers insurance or benefit or product. Examples of payers include an insurance company, healthcare professional (HMO), preferred provider organization (PPO), government agency (Medicaid, Medicare etc.) or any organization that may be contracted by one of these former groups.

**EDI Payroll Deducted and another group Premium Payment for Insurance Products (820)** is a transaction set for making a premium payment for insurance products. It can be used to order a financial institution to make a payment to a payee.

**EDI Health Care Eligibility/Benefit Inquiry (270)** is used to inquire about the health care benefits and eligibility associated with a subscriber or dependent.

**EDI Health Care Eligibility/Benefit Response (271)** is used to respond to a request inquiry about the health care benefits and eligibility associated with a subscriber or dependent.

**EDI Health Care Claim Status Request (276)** This transaction set can be used by a provider, recipient of health care products or services or their authorized agent to request the status of a health care claim.

**EDI Health Care Claim Status Notification (277)** This transaction set can be used by a healthcare payer or authorized agent to notify a provider, recipient or authorized agent regarding the status of a health care claim or encounter, or to request additional information from the provider regarding a health care claim or encounter. This transaction set is not intended to replace the Health Care Claim Payment/Advice Transaction Set (835) and therefore, is not used for account payment posting. The notification is at a summary or service line detail level. The notification may be solicited or unsolicited.

**EDI Health Care Service Review Information (278)** This transaction set can be used to transmit health care service information, such as subscriber, patient, demographic, diagnosis or treatment data for the purpose of the request for review, certification, notification or reporting the outcome of a health care services review.

**EDI Functional Acknowledgement Transaction Set (997)** this transaction set can be used to define the control structures for a set of acknowledgments to indicate the results of the syntactical analysis of the electronically encoded documents. Although it is not specifically named in the HIPAA Legislation or Final Rule, it is necessary for X12 transaction set processing. The encoded documents are the transaction sets, which are grouped in functional groups, used in defining transactions for business data interchange. This standard does not cover the semantic meaning of the information encoded in the transaction sets.

**Brief 5010 Transactions and Code Sets Rules Update Summary**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=10)]

1. Transaction Set (997) will be replaced by Transaction Set (999) "acknowledgment report".
2. The size of many fields {segment elements} will be expanded, causing a need for all IT providers to expand corresponding fields, element, files, GUI, paper media, and databases.
3. Some segments have been removed from existing Transaction Sets.
4. Many segments have been added to existing Transaction Sets allowing greater tracking and reporting of cost and patient encounters.
5. Capacity to use both "International Classification of Diseases" versions 9 (ICD-9) and 10 (ICD-10-CM) has been added.[[47]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-47)[[48]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-48)

**Security Rule**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=11)]

The Final Rule on Security Standards was issued on February 20, 2003. It took effect on April 21, 2003, with a compliance date of April 21, 2005, for most covered entities and April 21, 2006, for "small plans".[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications. Some privacy advocates have argued that this "flexibility" may provide too much latitude to covered entities.[[49]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-49) Software tools have been developed to assist covered entities in the risk analysis and remediation tracking. The standards and specifications are as follows:

* Administrative Safeguards – policies and procedures designed to clearly show how the entity will comply with the act
  + Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
  + The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
  + Procedures should clearly identify employees or classes of employees who have access to electronic protected health information (EPHI). Access to EPHI must be restricted to only those employees who have a need for it to complete their job function.
  + The procedures must address access authorization, establishment, modification, and termination.
  + Entities must show that an appropriate ongoing training program regarding the handling of PHI is provided to employees performing health plan administrative functions.
  + Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.
  + A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
  + Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
  + Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.
* Physical Safeguards – controlling physical access to protect against inappropriate access to protected data
  + Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.)
  + Access to equipment containing health information should be carefully controlled and monitored.
  + Access to hardware and software must be limited to properly authorized individuals.
  + Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
  + Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
  + If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.
* Technical Safeguards – controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.
  + Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
  + Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
  + Data corroboration, including the use of a checksum, double-keying, message authentication, and digital signature may be used to ensure data integrity.
  + Covered entities must also authenticate entities with which they communicate. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include password systems, two or three-way handshakes, telephone callback, and token systems.
  + Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
  + In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
  + Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non-health purposes.)

**Unique Identifiers Rule (National Provider Identifier)**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=12)]

HIPAA covered entities such as providers completing electronic transactions, healthcare clearinghouses, and large health plans must use only the National Provider Identifier (NPI) to identify covered healthcare providers in standard transactions by May 23, 2007. Small health plans must use only the NPI by May 23, 2008. Effective from May 2006 (May 2007 for small health plans), all covered entities using electronic communications (e.g., physicians, hospitals, health insurance companies, and so forth) must use a single new NPI. The NPI replaces all other identifiers used by health plans, Medicare, Medicaid, and other government programs.[[50]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-50) However, the NPI does not replace a provider's DEA number, state license number, or tax identification number. The NPI is 10 digits (may be alphanumeric), with the last digit being a checksum. The NPI cannot contain any embedded intelligence; in other words, the NPI is simply a number that does not itself have any additional meaning. The NPI is unique and national, never re-used, and except for institutions, a provider usually can have only one. An institution may obtain multiple NPIs for different "sub-parts" such as a free-standing cancer center or rehab facility.

**Enforcement Rule**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=13)]

On February 16, 2006, HHS issued the Final Rule regarding HIPAA enforcement. It became effective on March 16, 2006. The Enforcement Rule sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations. For many years there were few prosecutions for violations.[[51]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-51)

This may have changed with the fining of $50,000 to the Hospice of North Idaho (HONI) as the first entity to be fined for a potential HIPAA Security Rule breach affecting fewer than 500 people. Rachel Seeger, a spokeswoman for HHS, stated, "HONI did not conduct an accurate and thorough risk analysis to the confidentiality of ePHI as part of its security management process from 2005 through Jan. 17, 2012." This investigation was initiated with the theft from an employees vehicle of an unencrypted laptop containing 441 patient records.[[52]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-52)

|  |  |
| --- | --- |
|  | [Wikisource](https://en.wikipedia.org/wiki/Wikisource) has original text related to this article:  [**American Recovery and Reinvestment Act of 2009/Division A/Title XIII/Subtitle D**](https://en.wikisource.org/wiki/American_Recovery_and_Reinvestment_Act_of_2009/Division_A/Title_XIII/Subtitle_D) |

As of March 2013, the U.S. Dept. of Health and Human Services (HHS) has investigated over 19,306 cases that have been resolved by requiring changes in privacy practice or by corrective action. If noncompliance is determined by HHS, entities must apply corrective measures. Complaints have been investigated against many different types of businesses such as national pharmacy chains, major health care centers, insurance groups, hospital chains and other small providers. There were 9,146 cases where the HHS investigation found that HIPAA was followed correctly. There were 44,118 cases that HHS did not find eligible cause for enforcement; for example, a violation that started before HIPAA started; cases withdrawn by the pursuer; or an activity that does not actually violate the Rules. According to the HHS website,[[53]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-enf-53) the following lists the issues that have been reported according to frequency:

1. Misuse and disclosures of PHI
2. No protection in place of health information
3. Patient unable to access their health information
4. Using or disclosing more than the minimum necessary protected health information
5. No safeguards of electronic protected health information.

The most common entities required to take corrective action to be in voluntary compliance according to HHS are listed by frequency:[[53]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-enf-53)

1. Private Practices
2. Hospitals
3. Outpatient Facilities
4. Group plans such as insurance groups
5. Pharmacies

**Title III: Tax-related health provisions governing medical savings accounts**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=14)]

Title III standardizes the amount that may be saved per person in a [pre-tax medical savings account](https://en.wikipedia.org/wiki/Medical_savings_account_(United_States)). Beginning in 1997, medical savings account ("MSA") are available to employees covered under an employer-sponsored high deductible plan of a small employer and self-employed individuals.

**Title IV: Application and enforcement of group health insurance requirements**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=15)]

Title IV specifies conditions for group health plans regarding coverage of persons with pre-existing conditions, and modifies continuation of coverage requirements. It also clarifies continuation coverage requirements and includes [COBRA](https://en.wikipedia.org/wiki/Consolidated_Omnibus_Budget_Reconciliation_Act_of_1985) clarification.

**Title V: Revenue offset governing tax deductions for employers**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=16)]

Title V includes provisions related to company-owned life insurance for employers providing company-owned life insurance premiums, prohibiting the tax-deduction of interest on life insurance loans, company endowments, or contracts related to the company. It also repeals the financial institution rule to interest allocation rules. Finally, it amends provisions of law relating to [people who give up United States citizenship](https://en.wikipedia.org/wiki/List_of_former_United_States_citizens_who_relinquished_their_nationality) or permanent residence, expanding the [expatriation tax](https://en.wikipedia.org/wiki/Expatriation_tax) to be assessed against those deemed to be giving up their U.S. status for tax reasons, and making ex-citizens' names part of the [public record](https://en.wikipedia.org/wiki/Public_record) through the creation of the [Quarterly Publication of Individuals Who Have Chosen to Expatriate](https://en.wikipedia.org/wiki/Quarterly_Publication_of_Individuals_Who_Have_Chosen_to_Expatriate).[[54]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-54)

Effects on research and clinical care[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=17)]

The enactment of the Privacy and Security Rules has caused major changes in the way physicians and medical centers operate. The complex legalities and potentially stiff penalties associated with HIPAA, as well as the increase in paperwork and the cost of its implementation, were causes for concern among physicians and medical centers. An August 2006 article in the journal *Annals of Internal Medicine* detailed some such concerns over the implementation and effects of HIPAA.[[55]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-annals-55)

**Effects on research**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=18)]

HIPAA restrictions on researchers have affected their ability to perform retrospective, chart-based research as well as their ability to prospectively evaluate patients by contacting them for follow-up. A study from the [University of Michigan](https://en.wikipedia.org/wiki/University_of_Michigan) demonstrated that implementation of the HIPAA Privacy rule resulted in a drop from 96% to 34% in the proportion of follow-up surveys completed by study patients being followed after a [heart attack](https://en.wikipedia.org/wiki/Myocardial_infarction).[[56]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-56) Another study, detailing the effects of HIPAA on recruitment for a study on cancer prevention, demonstrated that HIPAA-mandated changes led to a 73% decrease in patient accrual, a tripling of time spent recruiting patients, and a tripling of mean recruitment costs.[[57]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-57)

In addition, [informed consent](https://en.wikipedia.org/wiki/Informed_consent) forms for research studies now are required to include extensive detail on how the participant's protected health information will be kept private. While such information is important, the addition of a lengthy, legalistic section on privacy may make these already complex documents even less user-friendly for patients who are asked to read and sign them.

These data suggest that the HIPAA privacy rule, as currently implemented, may be having negative impacts on the cost and quality of [medical research](https://en.wikipedia.org/wiki/Medical_research). Dr. Kim Eagle, professor of [internal medicine](https://en.wikipedia.org/wiki/Internal_medicine) at the University of Michigan, was quoted in the *Annals* article as saying, "Privacy is important, but research is also important for improving care. We hope that we will figure this out and do it right."[[55]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-annals-55)

**Effects on clinical care**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=19)]

The complexity of HIPAA, combined with potentially stiff penalties for violators, can lead physicians and medical centers to withhold information from those who may have a right to it. A review of the implementation of the HIPAA Privacy Rule by the U.S. Government Accountability Office found that health care providers were "uncertain about their legal privacy responsibilities and often responded with an overly guarded approach to disclosing information ... than necessary to ensure compliance with the Privacy rule".[[55]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-annals-55) Reports of this uncertainty continue.[[58]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-58)

**Costs of implementation**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=20)]

In the period immediately prior to the enactment of the HIPAA Privacy and Security Acts, medical centers and medical practices were charged with getting "into compliance". With an early emphasis on the potentially severe penalties associated with violation, many practices and centers turned to private, for-profit "HIPAA consultants" who were intimately familiar with the details of the legislation and offered their services to ensure that physicians and medical centers were fully "in compliance". In addition to the costs of developing and revamping systems and practices, the increase in paperwork and staff time necessary to meet the legal requirements of HIPAA may impact the finances of medical centers and practices at a time when insurance companies' and Medicare reimbursement is also declining.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**Education and training**[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=21)]

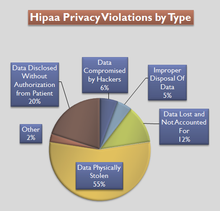
Education and training of healthcare providers is paramount to correct implementation of the HIPAA Privacy and Security Acts. Effective training must describe the statutory and regulatory background and purpose of HIPAA and a general summary of the principles and key provisions of the Privacy Rule.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]Although each HIPAA training course should be tailored towards the roles of employees attending the course, there are some vital elements that should be included:[[59]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-59)

* What is HIPAA?
* Why HIPAA is important?
* HIPAA Definitions
* Patient's rights
* HIPAA Privacy Rule
* Disclosures of PHI
* Breach Notifications
* BA Agreements
* HIPAA Security Rule
* Safeguarding ePHI
* Potential Violations
* Employee Sanctions

HIPAA acronym[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=22)]

Although HIPAA fits 1996 Public Law 104-191, *Health Insurance Portability and Accountability Act*, references to Title II's Privacy Rule are often stated as "Health Information Privacy and Portability Act (**HIPPA**)"[[60]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-COURT.HIPPA-60) by USA federal,[[61]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-61) state,[[62]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-62) county and other government sectors. Some governmental agencies have issued corrective followups regarding *HIPPA* and *HIPAA*.[[63]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-63)

Violations[[edit](https://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&action=edit&section=23)]

[](https://en.wikipedia.org/wiki/File:Hipaa_Violations_by_Type_-_Pie_Chart.png)

A breakdown of the HIPAA violations that resulted in the illegal exposure of personal information.

According to the US Department of Health and Human Services Office for Civil Rights, between April 2003 and January 2013, it received 91,000 complaints of HIPAA violations, in which 22,000 led to enforcement actions of varying kinds (from settlements to fines) and 521 led to referrals to the US Department of Justice as criminal actions.[[64]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-64) Examples of significant breaches of protected information and other HIPAA violations include:

* The largest loss of data that affected 4.9 million people by Tricare Management of Virginia in 2011[[65]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-65)
* The largest fines of $5.5 million levied against Memorial Healthcare Systems in 2017 for accessing confidential information of 115,143 patients[[66]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-66) and of $4.3 million levied against Cignet Health of Maryland in 2010 for ignoring patients' requests to obtain copies of their own records and repeated ignoring of federal officials' inquiries[[67]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-67)
* The first criminal indictment was lodged in 2011 against a Virginia physician who shared information with a patient's employer "under the false pretenses that the patient was a serious and imminent threat to the safety of the public, when in fact he knew that the patient was not such a threat."[[68]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-68)

According to Koczkodaj et al., 2018,[[69]](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#cite_note-69) the total number of individuals affected since October 2009 is 173,398,820.

The differences between civil and criminal penalties are summarized in the following table:

|  |  |  |
| --- | --- | --- |
| **Type of Violation** | **CIVIL Penalty (min)** | **CIVIL Penalty (max)** |
| Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA | $100 per violation, with an annual maximum of $25,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| HIPAA violation due to reasonable cause and not due to willful neglect | $1,000 per violation, with an annual maximum of $100,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| HIPAA violation due to willful neglect but violation is corrected within the required time period | $10,000 per violation, with an annual maximum of $250,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| HIPAA violation is due to willful neglect and is not corrected | $50,000 per violation, with an annual maximum of $1,000,000 | $50,000 per violation, with an annual maximum of $1.5 million |
| **Type of Violation** | **CRIMINAL Penalty** |  |
| Covered entities and specified individuals who "knowingly" obtain or disclose individually identifiable health information | A fine of up to $50,000  Imprisonment up to 1 year |  |
| Offenses committed under false pretenses | A fine of up to $100,000  Imprisonment up to 5 years |  |
| Offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm | A fine of up to $250,000  Imprisonment up to 10 years |  |

About FERC Industries: Natural Gas, Oil by Pipeline and Nuclear Energy

Federal Energy Regulatory Commission

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#p-search)

|  |  |
| --- | --- |
| **Federal Energy Regulatory Commission** | |
|  | |
| **Agency overview** | |
| **Formed** | October 1, 1977; 42 years ago |
| **Preceding** | * [Federal Power Commission](https://en.wikipedia.org/wiki/Federal_Power_Commission) |
| **Jurisdiction** | [U.S. government](https://en.wikipedia.org/wiki/Federal_government_of_the_United_States) |
| **Headquarters** | [Washington, D.C.](https://en.wikipedia.org/wiki/Washington,_D.C.), U.S. |
| **Agency executive** | * [Neil Chatterjee](https://en.wikipedia.org/wiki/Neil_Chatterjee), Chairman |
| **Parent agency** | [U.S. Department of Energy](https://en.wikipedia.org/wiki/United_States_Department_of_Energy) |
| **Website** | [www.FERC.gov](https://www.ferc.gov/) |

The **Federal Energy Regulatory Commission** (**FERC**) is the [United States](https://en.wikipedia.org/wiki/United_States) [federal agency](https://en.wikipedia.org/wiki/Independent_agencies_of_the_United_States_government) that regulates the transmission and wholesale sale of electricity and natural gas in interstate commerce and regulates the transportation of oil by pipeline in interstate commerce. FERC also reviews proposals to build interstate natural gas pipelines, natural gas storage projects, and [liquefied natural gas](https://en.wikipedia.org/wiki/Liquefied_natural_gas) (LNG) terminals, in addition to licensing non-federal hydropower projects.

FERC is composed of five commissioners who are nominated by the U.S. President and confirmed by the U.S. Senate. There may be no more than three commissioners of one political party serving on the commission at any given time.[[1]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-1)



**Contents**

* [1History](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#History)
  + [1.1Federal Power Commission](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Federal_Power_Commission)
  + [1.2Natural Gas Act of 1938](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Natural_Gas_Act_of_1938)
  + [1.3Birth of DOE; FPC Becomes FERC](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Birth_of_DOE;_FPC_Becomes_FERC)
  + [1.4Order 888](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Order_888)
  + [1.5Energy Policy Act of 2005](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Energy_Policy_Act_of_2005)
  + [1.6Order 1000](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Order_1000)
  + [1.7Order 841](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Order_841)
* [2FERC's primary duties](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#FERC's_primary_duties)
* [3Jurisdiction and authorities](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Jurisdiction_and_authorities)
* [4Commissioners](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Commissioners)
* [5Criticism](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Criticism)
  + [5.1Federal versus state authority](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Federal_versus_state_authority)
* [6See also](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#See_also)
  + [6.1Related legislation](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Related_legislation)
* [7References](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#References)
* [8Further reading](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#Further_reading)
* [9External links](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#External_links)

History[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=1)]

**Federal Power Commission**[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=2)]

The [Federal Power Commission](https://en.wikipedia.org/wiki/Federal_Power_Commission) (FPC), which preceded FERC, was established by Congress in 1920 to allow cabinet members to coordinate federal hydropower development.

In 1935, the FPC was transformed into an [independent regulatory agency](https://en.wikipedia.org/wiki/Independent_agencies_of_the_United_States_government) with five members nominated by the [President](https://en.wikipedia.org/wiki/President_of_the_United_States) and confirmed by the [Senate](https://en.wikipedia.org/wiki/United_States_Senate). The FPC was authorized to regulate both hydropower and interstate electricity.

**Natural Gas Act of 1938**[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=3)]

In 1938, the [Natural Gas Act](https://en.wikipedia.org/wiki/Natural_Gas_Act) gave FPC jurisdiction over interstate natural gas pipelines and wholesale sales. In 1942, this jurisdiction was expanded to cover the licensing of more natural gas facilities. In 1954, the Supreme Court decision in [*Phillips Petroleum Co. v. Wisconsin*](https://en.wikipedia.org/wiki/Phillips_Petroleum_Co._v._Wisconsin) extended FPC jurisdiction over all wellhead sales of natural gas in interstate commerce.

**Birth of DOE; FPC Becomes FERC**[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=4)]

In response to the [1973 oil crisis](https://en.wikipedia.org/wiki/1973_oil_crisis), [Congress](https://en.wikipedia.org/wiki/United_States_Congress) passed the Department of Energy Organization Act in 1977, to consolidate various energy-related agencies into a [Department of Energy](https://en.wikipedia.org/wiki/United_States_Department_of_Energy). Congress insisted that a separate independent regulatory body be retained, and the FPC was renamed the Federal Energy Regulatory Commission (FERC), preserving its independent status within the Department.[[2]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-2) Its most basic mandate was to “determine whether wholesale electricity prices were unjust and unreasonable and, if so, to regulate pricing and order refunds for overcharges to ratepayers.”[[3]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-3) FERC was also given added responsibility to hear appeals of DOE oil price control determinations and to conduct all "on the record" hearings for DOE.[[4]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-4) As a result, DOE does not have any [administrative law judges](https://en.wikipedia.org/wiki/Administrative_law_judge). As a further protection, when the Department of Energy proposes a rule, it must refer the proposal to FERC, and FERC can take over the proceeding if FERC determines that the rulemaking "may significantly affect" matters in its jurisdiction.[[5]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-5) The DOE Act also transferred the regulation of interstate oil pipelines from the [Interstate Commerce Commission](https://en.wikipedia.org/wiki/Interstate_Commerce_Commission) to FERC.[[6]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-6) However, the FERC lost some jurisdiction over the imports and exports of gas and electricity.

In 1978, FERC was given additional responsibilities for harmonizing the regulation of wellhead gas sales in both the intrastate and interstate markets. FERC also administered a program to foster new [cogeneration](https://en.wikipedia.org/wiki/Cogeneration) and small power production under the [Public Utilities Regulatory Policy Act of 1978](https://en.wikipedia.org/wiki/Public_Utility_Regulatory_Policies_Act), which was passed as part of the [National Energy Act of 1978](https://en.wikipedia.org/wiki/National_Energy_Act). The National Energy Act included the Natural Gas Policy Act, which reduced the scope of federal price regulation, to bring greater competition to both the natural gas and electric industry.

In 1989, Congress ended federal regulation of wellhead natural gas prices, with the passage of the Natural Gas Wellhead Decontrol Act of 1989.[[7]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-7)

**Order 888**[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=5)]

In 1996, FERC issued Order 888, which spurred the creation of [regional transmission organizations](https://en.wikipedia.org/wiki/Regional_transmission_organization) in the United States. This would impact existing electric power pools by rebranding themselves as independent transmission operators. Electric utilities in some regions began to spin off their generation units as separate companies that would compete in a wholesale electric market administered by the RTOs.[[8]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-8)

**Energy Policy Act of 2005**[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=6)]

In 2001, the G.W. Bush administration sought to give the authority of eminent domain to FERC to circumvent state and local bureaucratic processed which often slowed the siting of new transmission projects. This expansion of power was most fiercely opposed by Bush’s own Republican party as being an expansion of federal power.  Legal battles over the issue ended with the 2005 Energy Bill (Energy Policy Act of 2005) which was passed with approval of Democrats and Republicans.

The [Energy Policy Act of 2005](https://en.wikipedia.org/wiki/Energy_Policy_Act_of_2005) expanded FERC's authority to protect the reliability and cybersecurity of the bulk power system through the establishment and enforcement of mandatory standards, as well as greatly expanding FERC authority to impose civil [penalties](https://en.wikipedia.org/wiki/Sanctions_(law)) on entities that manipulate the electricity and natural gas markets. The Energy Policy Act of 2005 also gave FERC additional responsibilities and authority. Among the many provisions of the law, FERC was given what is known as “backstop” siting authority which allows FERC to overrule any denial of transmission projects by a state within established corridors of transmission congestion "to expand transmission in limited regions of the country facing transmission constraints." [[9]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-9)[[10]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-10)

**Order 1000**[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=7)]

In 2010, FERC issued Order 1000, which required RTOs to create regional transmission plans and identify transmission needs based on public policy. Cost allocation reforms were included, possibly to reduce barriers faced by nonincumbent transmission developers.[[11]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-11)

**Order 841**[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=8)]

In 2018, FERC issued Order 841, which required wholesale markets to open up to individual storage installations, regardless of interconnection point (transmission, distribution or behind-the-meter).[[12]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-12)[[13]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-13)

FERC's primary duties[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=9)]

The responsibilities of FERC include the following:

* Regulating the transmission and sale of natural gas for resale in [interstate commerce](https://en.wikipedia.org/wiki/Interstate_commerce);
* Regulating the transmission of oil by pipelines in interstate commerce;
* Regulating the transmission and wholesale sales of electricity in interstate commerce;
* Licensing and inspecting private, municipal, and state hydroelectric projects;
* Approving the siting of and abandonment of interstate natural gas facilities, including pipelines, storage and [liquefied natural gas](https://en.wikipedia.org/wiki/Liquefied_natural_gas);
* Ensuring the reliability of high voltage interstate transmission system;
* Monitoring and investigating energy markets;
* Using civil penalties and other means against energy organizations and individuals who violate FERC rules in the energy markets;
* Overseeing environmental matters related to natural gas and hydroelectricity projects and major electricity policy initiatives; and
* Administering accounting and financial reporting regulations and regulating businesses of regulated companies.

Jurisdiction and authorities[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=10)]

FERC is an [independent regulatory agency](https://en.wikipedia.org/wiki/Independent_agencies_of_the_United_States_government) within the [United States Department of Energy](https://en.wikipedia.org/wiki/United_States_Department_of_Energy). The [President](https://en.wikipedia.org/wiki/President_of_the_United_States) and [Congress](https://en.wikipedia.org/wiki/United_States_Congress) do not generally review FERC decisions, but the decisions are reviewable by the [federal courts](https://en.wikipedia.org/wiki/United_States_federal_courts). FERC is self-funding, in that Congress sets its budget through annual and supplemental appropriations and FERC is authorized to raise revenue to reimburse the United States Treasury for its appropriations, through annual charges to the natural gas, oil, and electric industries it regulates.[[14]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-14)

FERC is independent of the Department of Energy because FERC activities "shall not be subject to further view by the Secretary [of Energy] or any officer or employee of the Department".[[15]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-15) The Department of Energy can, however, participate in FERC proceedings as a third party.

FERC is composed of up to five commissioners who are appointed by the President and confirmed by the Senate. The President appoints one of the commissioners to be the chairman of FERC, the administrative head of the agency. FERC is a bipartisan body; no more than three commissioners may be of the same political party.

FERC has promoted voluntary formation of [Regional Transmission Organizations](https://en.wikipedia.org/wiki/Regional_transmission_organization) (RTOs) and [Independent System Operators](https://en.wikipedia.org/wiki/Independent_System_Operator) (ISOs) to eliminate the potential for undue discrimination in access to the [electric grid](https://en.wikipedia.org/wiki/Electric_grid); regional and interregional transmission planning and cost allocation through the landmark Order No. 1000.

FERC investigated the alleged manipulation of [electricity market](https://en.wikipedia.org/wiki/Electricity_market) by [Enron](https://en.wikipedia.org/wiki/Enron_Corporation) and other energy companies, and their role in the [California electricity crisis](https://en.wikipedia.org/wiki/California_electricity_crisis). FERC has collected more than $6.3 billion from California electric market participants through settlements. Since passage of the Energy Policy Act of 2005, FERC has imposed, through settlements and orders, more than $1 billion in civil penalties and disgorgement of unjust profits to address violations of its anti-[market manipulation](https://en.wikipedia.org/wiki/Market_manipulation) and other rules.

FERC regulates approximately 1,600 hydroelectric projects in the U.S. It is largely responsible for permitting construction of a large network of interstate natural gas pipelines. FERC also works closely with the [United States Coast Guard](https://en.wikipedia.org/wiki/United_States_Coast_Guard) to review the safety, security, and environmental impacts of proposed LNG terminals and associated shipping.

Commissioners[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=11)]

The Commissioners are:

| **Name** | **Title** | **Party** | **Took office** | **Term expires** |
| --- | --- | --- | --- | --- |
| [Neil Chatterjee](https://en.wikipedia.org/wiki/Neil_Chatterjee) | Chairman | Republican | August 8, 2017 | June 30, 2021 |
| [Richard Glick](https://en.wikipedia.org/wiki/Richard_Glick) | Commissioner | Democrat | November 29, 2017 | June 30, 2022 |
| [Bernard McNamee](https://en.wikipedia.org/wiki/Bernard_McNamee) | Commissioner | Republican | December 11, 2018 | June 30, 2020 |

Criticism[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=12)]

FERC has been subject to criticism and increasing acts of activism by people from communities affected by Commission decisions approving pipeline and related projects.[[16]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-auto-16) They contend that FERC "blithely greenlights too many pipelines, export terminals and other gas infrastructure"[[16]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-auto-16) and that FERC's structure in which it recovers its annual operating costs directly from the entities it regulates creates bias in favor of the issuance of pipeline certificates.[[17]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-auto1-17) Some of these critics have disrupted several regular open meetings of the Commission,[[18]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-18) and they staged two, week-long blockades of the Commission's headquarters in Washington, D.C., to make their points.[[19]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-19) "Pipelines are facing unprecedented opposition," Commissioner LaFleur remarked to the National Press Club in a 2015 speech. "We have a situation here."[[20]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-20)[[21]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-21)[[22]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-22)

FERC's decisions in these cases are often upheld by the courts. In a July 1, 2014, decision, *No Gas Pipeline v. Federal Energy Regulatory Commission*, the United States Court of Appeals for the District of Columbia Circuit (D.C. Circuit) said that pipeline applicants are not likely to pursue many certificates that are hopeless. "The fact that they generally succeed in choosing to expend their resources on applications that serve their own financial interests does not mean that an agency which recognizes merit in such applications is biased," the court said.[[23]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-23) Others have directly disputed FERC's critics by pointing out that "FERC is a creature of law. It follows a careful administrative path to regulate only a portion of natural gas such as interstate pipelines and LNG import and export terminals. That regulation includes extensive environmental review, driven by many federal laws enacted by Congress, signed by the president, and reviewed and upheld by the U.S. Supreme Court. If the agency were to adopt the path [suggested by these critics], FERC's decisions would routinely be overturned by the federal courts."[[24]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-24)

The United States District Court for the District of Columbia also dismissed a case involving allegations of structural bias on the part of FERC. The plaintiffs contended that the Omnibus Budget Act of 1986 funding mechanism requires the Commission to recover its budget through proportional charges on regulated entities, therefore making FERC biased in favor of the industry from which it gets its funding. But in an order issued March 22, 2017, the court said the plain language of the statute indicates that FERC does not have control over its own budget. "The Commission's budget cannot be increased by approving pipelines; rather, [the statute] requires the Commission to make adjustments to 'eliminate any overrecovery or underrecovery.' If Plaintiffs are unhappy with Congress's chosen appropriations to the Commission…, Plaintiffs' recourse lies with their legislative representatives."[[17]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-auto1-17)

In New Jersey, the FERC approval of the [PennEast Pipeline](https://en.wikipedia.org/wiki/PennEast_Pipeline) was met with widespread criticism by environmental groups who called the decision highly partisan. "FERC has once again demonstrated its tremendous bias for, and partnership with, the pipeline industry," said Maya van Rossum, leader of the Delaware Riverkeeper Network. Doug O'Malley, president of Environment New Jersey, called the FERC approval of the pipeline a "disaster." [David Pringle](https://en.wikipedia.org/w/index.php?title=David_Pringle_(activist)&action=edit&redlink=1), state campaign director of [Clean Water Action](https://en.wikipedia.org/wiki/Clean_Water_Action) and 2018 Congressional candidate, suggested the FERC was serving a partisan interest over the interests of the people of New Jersey, suggesting "The FERC needs to remember it works for the people of the United States not PennEast." [[25]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-25) These criticisms were unfounded as the D.C. Circuit Court of Appeals on July 10, 2018, rejected the Delaware Riverkeeper Network and Maya Van Rossum’s claim that FERC has an incentive to award pipeline certificates because it collects its operating expenses from regulated parties. Upholding a lower court ruling, the D.C. Circuit also rejected the Delaware Riverkeeper Network’s challenge to FERC’s use of tolling orders to meet its statutory deadlines for acting on rehearing applications.[[26]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-26)

However, the D.C. Circuit has provided additional guidance concerning Commission procedures, stating that in one case FERC failed to consider the cumulative environmental impact of four projects that had been separately proposed by the same pipeline. The D.C. Circuit held that the projects were not financially independent and were "a single pipeline" that was "linear and physically interdependent," so the cumulative environmental impacts should have been considered concurrently.[[27]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-27) Subsequently, in a separate decision, the D.C. Circuit sustained the Commission's conduct of separate environmental assessments when it clarified that the "critical" factor was that all of the pipeline's projects were either under construction or pending before FERC for environmental review at the same time, noting that the projects lacked temporal overlap.[[28]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-28) Furthermore, in another case, the D.C. Circuit sustained the Commission's use of a separate environmental assessment when it reasoned that the projects in dispute were "unrelated" and did not depend on one another for their justification.[[29]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-29) This guidance has allowed FERC to address additional claims of improper segmentation.[[30]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-30)

FERC's leaders have stressed many times since the onset of the increased activism that the proper way to oppose a proposed new infrastructure project is by participating in the related proceeding by submitting comments and participating in public comment sessions, site visits and scoping meetings, since FERC decisions can be appealed up to the Supreme Court.

**Federal versus state authority**[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=13)]

There are regions of the country where the state public utility commission and the FERC regulated Regional Transmission Organization operate in identical footprints (e.g., [New York](https://en.wikipedia.org/wiki/New_York_energy_law)). Where this occurs, state policy makers and FERC frequently clash as to the extent of federal power and influence within the state.

The planning and siting of public policy and renewable power plants and merchant transmission lines can be contentious because the planning process must proceed through both entities. For example in New York, any large (>20 MW for the NYISO and >25 MW for the state Siting Committee) generation or merchant transmission facility must proceed through both the planning process of the NYISO - which operates on a two-year cycle at minimum with an inclusive class year pool of new projects evaluated simultaneously - and the siting process of the state Board on Electric Siting and the Environment. Prior to the formation of the NYISO, the planning process was mostly determined by the state siting board (although the utilities' [power pool](https://en.wikipedia.org/wiki/Power_pool) might have had their own closed door planning session) and large generation projects were developed by the utilities themselves.[[31]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-31)[[32]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-32) This dual planning process provides an opportunity for other market participants to drag out the process legally, not including the other state and/or federal environmental, trade (if an international connection with Canada is requested) and local certification and regulation processes that need to be met.

This controversy similarly applies to various electric wholesale-market issues within the RTO, i.e., when a state public utility commission asserts that its retail ratepayers (under state regulation) will be impacted by wholesale-market stakeholder decisions and reforms (under federal-level regulation). In contrast, prior to the formation of the NYISO in 1999 in New York, wholesale energy prices were set within a utility's state rate case proceeding. Examples of contentious issues in New York include the NYISO's development of buyer-side mitigation (price floors) in its capacity market,[[33]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-33) proxy peaking-unit specifications during the demand-curve reset (that helps set capacity market prices),[[34]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-34)[[35]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-35) the state's granting of zero-emissions credits to wholesale-market participating nuclear power plants,[[36]](https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission#cite_note-36) and the [creation of a new capacity zone amidst state and transmission owner policy initiatives](https://en.wikipedia.org/wiki/Transmission_Owner_Transmission_Solutions#New_capacity_zone).

See also[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=14)]

* [Category:Federal Energy Regulatory Commission chairpersons](https://en.wikipedia.org/wiki/Category:Federal_Energy_Regulatory_Commission_chairpersons)
* [21st-century fossil fuel regulations in the United States](https://en.wikipedia.org/wiki/21st-century_fossil_fuel_regulations_in_the_United_States)
* [Custody transfer](https://en.wikipedia.org/wiki/Custody_transfer)
* [High-voltage direct current](https://en.wikipedia.org/wiki/High-voltage_direct_current)
* [North American Electric Reliability Corporation](https://en.wikipedia.org/wiki/North_American_Electric_Reliability_Corporation) (NERC)
* [United States energy law](https://en.wikipedia.org/wiki/United_States_energy_law)

**Related legislation**[[edit](https://en.wikipedia.org/w/index.php?title=Federal_Energy_Regulatory_Commission&action=edit&section=15)]

* [Collinsville Renewable Energy Promotion Act (H.R. 316;113th Congress)](https://en.wikipedia.org/wiki/Collinsville_Renewable_Energy_Promotion_Act_(H.R._316;113th_Congress)) – proposed law ordering the FERC to reinstate two project licenses for a town in Connecticut
* [Hydropower Regulatory Efficiency Act of 2013 (H.R. 267; 113th Congress)](https://en.wikipedia.org/wiki/Hydropower_Regulatory_Efficiency_Act_of_2013_(H.R._267;_113th_Congress)) – proposed law that will alter the regulations the FERC is charged with enforcing
* [*Scenic Hudson Preservation Conference v. Federal Power Commission*](https://en.wikipedia.org/wiki/Scenic_Hudson_Preservation_Conference_v._Federal_Power_Commission) - "Birth" of the environmental movement in the United States
* [Title 18 of the Code of Federal Regulations](https://en.wikipedia.org/wiki/Title_18_of_the_Code_of_Federal_Regulations)

About GLBA Industries: Financial

<https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act>

*GLBA" redirects here. It is not to be confused with*[*GBLA (disambiguation)*](https://en.wikipedia.org/wiki/GBLA_(disambiguation))*.*

|  |  |
| --- | --- |
| **Gramm–Leach–Bliley Act** | |
| [Great Seal of the United States](https://en.wikipedia.org/wiki/File:Great_Seal_of_the_United_States_(obverse).svg) | |
| **Other short titles** | * Federal Home Loan Bank System Modernization Act of 1999 * Financial Services Modernization Act of 1999 * Prime Act * Program for Investment in Microentrepreneurs Act of 1999 |
| **Long title** | An Act to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, and other financial service providers, and for other purposes. |
| [**Acronyms**](https://en.wikipedia.org/wiki/Acronym)(colloquial) | GLBA |
| **Nicknames** | glibba, ATM Fee Reform Act of 1999 |
| **Enacted by** | the [106th United States Congress](https://en.wikipedia.org/wiki/106th_United_States_Congress) |
| **Effective** | November 12, 1999 |
| **Citations** | |
| **Public law** | [106–102](http://www.gpo.gov/fdsys/pkg/STATUTE-113/pdf/STATUTE-113-Pg1338.pdf) |
| [**Statutes at Large**](https://en.wikipedia.org/wiki/United_States_Statutes_at_Large) | 113 [Stat.](https://en.wikipedia.org/wiki/United_States_Statutes_at_Large) [1338](http://legislink.org/us/stat-113-1338) |
| **Codification** | |
| **Acts repealed** | [Glass–Steagall Act](https://en.wikipedia.org/wiki/Glass%E2%80%93Steagall_Act) |
| **Titles amended** | * [12 U.S.C.: Banks and Banking](https://en.wikipedia.org/wiki/Title_12_of_the_United_States_Code) * [15 U.S.C.: Commerce and Trade](https://en.wikipedia.org/wiki/Title_15_of_the_United_States_Code) |
| [**U.S.C.**](https://en.wikipedia.org/wiki/United_States_Code)**sections created** | [12 U.S.C.](https://en.wikipedia.org/wiki/Title_12_of_the_United_States_Code) [§ 24a](https://www.law.cornell.edu/uscode/text/12/24a), [§ 248b](https://www.law.cornell.edu/uscode/text/12/248b), [§ 1831v](https://www.law.cornell.edu/uscode/text/12/1831v), [§ 1831w](https://www.law.cornell.edu/uscode/text/12/1831w), [§ 1831x](https://www.law.cornell.edu/uscode/text/12/1831x), [§ 1831y](https://www.law.cornell.edu/uscode/text/12/1831y), [§ 1848a](https://www.law.cornell.edu/uscode/text/12/1848a), [§ 2908](https://www.law.cornell.edu/uscode/text/12/2908) [15 U.S.C.](https://en.wikipedia.org/wiki/Title_15_of_the_United_States_Code) [§ 80b-10a](https://www.law.cornell.edu/uscode/text/15/80b-10a) |
| **U.S.C. sections amended** | [12 U.S.C.](https://en.wikipedia.org/wiki/Title_12_of_the_United_States_Code) [§ 78](https://www.law.cornell.edu/uscode/text/12/78), [§ 377](https://www.law.cornell.edu/uscode/text/12/377) [15 U.S.C.](https://en.wikipedia.org/wiki/Title_15_of_the_United_States_Code) [§ 80](https://www.law.cornell.edu/uscode/text/15/80) |
| [**Legislative history**](http://thomas.loc.gov/cgi-bin/bdquery/z?d106:SN00900:@@@R) | |
| * **Introduced in the Senate** **as** [S. 900](https://www.congress.gov/bill/106th-congress/senate-bill/900) **by** [Phil Gramm](https://en.wikipedia.org/wiki/Phil_Gramm) ([R](https://en.wikipedia.org/wiki/Republican_Party_(United_States))-[TX](https://en.wikipedia.org/wiki/Texas)) **on** April 28, 1999 * **Committee consideration by** [Committee on Banking, Housing, and Urban Affairs](https://en.wikipedia.org/wiki/United_States_Senate_Committee_on_Banking,_Housing,_and_Urban_Affairs) * **Passed the Senate on** May 6, 1999 ([54-44](https://www.govtrack.us/congress/votes/106-1999/s105)) * **Passed the House as the**Financial Services Act of 1999**on** July 1, 1999 ([343-86](http://clerk.house.gov/evs/1999/roll276.xml)) * **Reported by the joint conference committee on** November 2, 1999; **agreed to by the Senate on** November 4, 1999 ([90-8](https://www.govtrack.us/congress/votes/106-1999/s354)) **and by the House on** November 4, 1999 ([362-57](https://www.govtrack.us/congress/votes/106-1999/h570)) * **Signed into law by President** [Bill Clinton](https://en.wikipedia.org/wiki/Bill_Clinton) **on** November 12, 1999 | |

The **Gramm–Leach–Bliley Act** (**GLBA**), also known as the **Financial Services Modernization Act of 1999**, ([Pub.L.](https://en.wikipedia.org/wiki/Act_of_Congress) [106–102](http://legislink.org/us/pl-106-102), 113 [Stat.](https://en.wikipedia.org/wiki/United_States_Statutes_at_Large) [1338](http://legislink.org/us/stat-113-1338), enacted November 12, 1999) is an [act](https://en.wikipedia.org/wiki/Act_of_Congress) of the [106th United States Congress](https://en.wikipedia.org/wiki/106th_United_States_Congress) (1999–2001). It repealed part of the [Glass–Steagall Act of 1933](https://en.wikipedia.org/wiki/Glass%E2%80%93Steagall_Legislation), removing barriers in the market among [banking](https://en.wikipedia.org/wiki/Bank) companies, [securities](https://en.wikipedia.org/wiki/Security_(finance)) companies and [insurance](https://en.wikipedia.org/wiki/Insurance) companies that prohibited any one institution from acting as any combination of an [investment bank](https://en.wikipedia.org/wiki/Investment_bank), a [commercial bank](https://en.wikipedia.org/wiki/Commercial_bank), and an [insurance company](https://en.wikipedia.org/wiki/Insurance_company). With the bipartisan passage of the [Gramm](https://en.wikipedia.org/wiki/Phil_Gramm)–[Leach](https://en.wikipedia.org/wiki/Jim_Leach)–[Bliley](https://en.wikipedia.org/wiki/Thomas_J._Bliley_Jr.) Act, commercial banks, investment banks, securities firms, and insurance companies were allowed to consolidate. Furthermore, it failed to give to the SEC or any other financial regulatory agency the authority to regulate large investment bank holding companies.[[1]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-1) The legislation was signed into law by President [Bill Clinton](https://en.wikipedia.org/wiki/Bill_Clinton).[[2]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-2)

A year before the law was passed, [Citicorp](https://en.wikipedia.org/wiki/Citicorp), a commercial bank [holding company](https://en.wikipedia.org/wiki/Holding_company), merged with the insurance company [Travelers Group](https://en.wikipedia.org/wiki/Travelers_Group) in 1998 to form the conglomerate [Citigroup](https://en.wikipedia.org/wiki/Citigroup), a corporation combining banking, securities and insurance services under a house of brands that included [Citibank](https://en.wikipedia.org/wiki/Citibank), [Smith Barney](https://en.wikipedia.org/wiki/Smith_Barney), [Primerica](https://en.wikipedia.org/wiki/Primerica), and [Travelers](https://en.wikipedia.org/wiki/Travelers_Insurance_Corporation). Because this merger was a violation of the Glass–Steagall Act and the [Bank Holding Company Act of 1956](https://en.wikipedia.org/wiki/Bank_Holding_Company_Act), the [Federal Reserve](https://en.wikipedia.org/wiki/Federal_Reserve) gave Citigroup a temporary waiver in September 1998.[[3]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-broome-3) Less than a year later, GLBA was passed to legalize these types of mergers on a permanent basis. The law also repealed Glass–Steagall's conflict of interest prohibitions "against simultaneous service by any officer, director, or employee of a securities firm as an officer, director, or employee of any member bank".[[4]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-4)

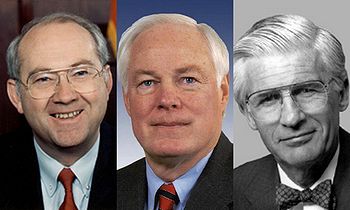


**Contents**

* [1Legislative history](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Legislative_history)
* [2Changes caused by the Act](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Changes_caused_by_the_Act)
* [3Remaining restrictions](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Remaining_restrictions)
* [4Privacy](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Privacy)
* [5Financial Privacy Rule](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Financial_Privacy_Rule)
  + [5.1Financial institutions](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Financial_institutions)
  + [5.2Consumer vs. customer defined](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Consumer_vs._customer_defined)
  + [5.3Consumer/client privacy rights](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Consumer/client_privacy_rights)
* [6Receipt of GLBA notices by consumers](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Receipt_of_GLBA_notices_by_consumers)
  + [6.1Service of notice requirements](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Service_of_notice_requirements)
  + [6.2Response to receipt of a GLBA notice](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Response_to_receipt_of_a_GLBA_notice)
* [7Synergy between GLBA and GDPR](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Synergy_between_GLBA_and_GDPR)
* [8Safeguards Rule](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Safeguards_Rule)
* [9Pretexting protection](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Pretexting_protection)
* [10Effect on usury law](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Effect_on_usury_law)
* [11Controversy](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Controversy)
  + [11.1Criticisms](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Criticisms)
* [12Amendments](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Amendments)
  + [12.1Proposed](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Proposed)
* [13See also](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#See_also)
* [14Notes](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Notes)
* [15References](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#References)
* [16Sources](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Sources)
* [17External links](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#External_links)
  + [17.1Compliance information](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Compliance_information)
  + [17.2Consumer/client rights information](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Consumer/client_rights_information)
  + [17.3History of the GLB](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#History_of_the_GLB)
  + [17.4Congressional voting records on Gramm–Leach–Bliley Act](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Congressional_voting_records_on_Gramm%E2%80%93Leach%E2%80%93Bliley_Act)

Legislative history[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=1)]

The banking industry had been seeking the repeal of the 1933 Glass–Steagall Act since the 1980s, if not earlier.[[5]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-5)[[6]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-6) In 1987 the [Congressional Research Service](https://en.wikipedia.org/wiki/Congressional_Research_Service) prepared a report that explored the cases for and against preserving the Glass–Steagall act.[[7]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-7)

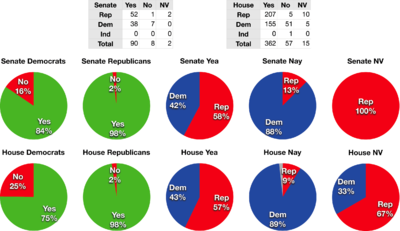
[](https://en.wikipedia.org/wiki/File:GrammLeachBliley.jpg)

[Sen.](https://en.wikipedia.org/wiki/United_States_Senate) [Phil Gramm](https://en.wikipedia.org/wiki/Phil_Gramm) ([R](https://en.wikipedia.org/wiki/Republican_Party_(United_States)), [Texas](https://en.wikipedia.org/wiki/List_of_United_States_Senators_from_Texas)), [Rep.](https://en.wikipedia.org/wiki/United_States_House_of_Representatives) [Jim Leach](https://en.wikipedia.org/wiki/Jim_Leach) ([R](https://en.wikipedia.org/wiki/Republican_Party_(United_States)), [Iowa](https://en.wikipedia.org/wiki/Iowa%27s_2nd_congressional_district)), and Rep. [Thomas J. Bliley, Jr.](https://en.wikipedia.org/wiki/Thomas_J._Bliley,_Jr.) ([R](https://en.wikipedia.org/wiki/Republican_Party_(United_States)), [Virginia](https://en.wikipedia.org/wiki/Virginia%27s_7th_congressional_district)), the co-sponsors of the Gramm–Leach–Bliley Act.

Respective versions of the Financial Services Act were introduced in the [U.S. Senate](https://en.wikipedia.org/wiki/U.S._Senate) by [Phil Gramm](https://en.wikipedia.org/wiki/Phil_Gramm) ([Republican](https://en.wikipedia.org/wiki/Republican_Party_(United_States)) of Texas) and in the [U.S. House of Representatives](https://en.wikipedia.org/wiki/U.S._House_of_Representatives) by [Jim Leach](https://en.wikipedia.org/wiki/Jim_Leach) (R-Iowa). The third lawmaker associated with the bill was Rep. [Thomas J. Bliley, Jr.](https://en.wikipedia.org/wiki/Thomas_J._Bliley,_Jr.) (R-Virginia), Chairman of the [House Commerce Committee](https://en.wikipedia.org/wiki/House_Commerce_Committee) from 1995 to 2001.

During debate in the [House of Representatives](https://en.wikipedia.org/wiki/House_of_Representatives_(United_States)), Rep. [John Dingell](https://en.wikipedia.org/wiki/John_Dingell) ([Democrat](https://en.wikipedia.org/wiki/Democratic_Party_(United_States)) of Michigan) argued that the bill would result in banks becoming "too big to fail." Dingell further argued that this would necessarily result in a bailout by the Federal Government.[[8]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-8)

The House passed its version of the *Financial Services Act of 1999* on July 1, 1999, by a bipartisan vote of 343–86 (Republicans 205–16; Democrats 138–69; [Independent](https://en.wikipedia.org/wiki/Bernie_Sanders) 0–1),[[9]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-HR10.EH-9)[[10]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-HR10.ACTIONS-10)[[note 1]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-12) two months after the Senate had already passed its version of the bill on May 6 by a much narrower 54–44 vote along basically partisan lines (53 Republicans and 1 Democrat in favor; 44 Democrats opposed).[[12]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-S900.ES-13)[[13]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-S900.ACTIONS-14)[[14]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-106-105.ES-15)[[note 2]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-16)

[](https://en.wikipedia.org/wiki/File:Gramm-Leach-Bliley_Vote_1999.png)

Final Congressional vote by chamber and party, November 4, 1999

When the two chambers could not agree on a joint version of the bill, the House voted on July 30 by a vote of 241–132 (R 58–131; D 182–1; Ind. 1–0) to instruct its negotiators to work for a law which ensured that consumers enjoyed medical and financial privacy as well as "robust competition and equal and non-discriminatory access to financial services and economic opportunities in their communities" (i.e., protection against exclusionary [redlining](https://en.wikipedia.org/wiki/Redlining)).[[note 3]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-18)

The bill then moved to a joint [conference committee](https://en.wikipedia.org/wiki/United_States_congressional_conference_committee) to work out the differences between the Senate and House versions. Democrats agreed to support the bill after Republicans agreed to strengthen provisions of the anti-redlining [Community Reinvestment Act](https://en.wikipedia.org/wiki/Community_Reinvestment_Act) and address certain privacy concerns; the conference committee then finished its work by the beginning of November.[[16]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-Veto_Promise-19)[[17]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-NHI-CRA-20) On November 4, the final bill resolving the differences was passed by the Senate 90–8,[[18]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-106-354.EH-21)[[note 4]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-22) and by the House 362–57.[[19]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-106-570.EH-23)[[note 5]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-24) The legislation was signed into law by President [Bill Clinton](https://en.wikipedia.org/wiki/Bill_Clinton) on November 12, 1999.[[20]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-25)

Changes caused by the Act[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=2)]

Many of the largest banks, brokerages, and insurance companies desired the Act at the time. The justification was that individuals usually put more money into investments when the economy is doing well, but they put most of their money into [savings accounts](https://en.wikipedia.org/wiki/Savings_account) when the economy turns bad. With the new Act, they would be able to do both 'savings' and 'investment' at the same financial institution, which would be able to do well in both good and bad economic times.

Prior to the Act, most financial services companies were already offering both saving and investment opportunities to their customers. On the retail/consumer side, a bank called [Norwest Corporation](https://en.wikipedia.org/wiki/Norwest_Corporation), which would later merge with [Wells Fargo Bank](https://en.wikipedia.org/wiki/Wells_Fargo_Bank), led the charge in offering all types of financial services products in 1986. [American Express](https://en.wikipedia.org/wiki/American_Express) attempted to own participants in almost every field of financial business (although there was little [synergy](https://en.wikipedia.org/wiki/Corporate_synergy) among them). Things culminated in 1998 when Citibank merged with [The Travelers Companies](https://en.wikipedia.org/wiki/The_Travelers_Companies), creating [Citigroup](https://en.wikipedia.org/wiki/Citigroup). The merger violated the [Bank Holding Company Act](https://en.wikipedia.org/wiki/Bank_Holding_Company_Act) (BHCA), but Citibank was given a two-year forbearance that was based on an assumption that they would be able to force a change in the law. The Gramm–Leach–Bliley Act passed in November 1999, repealing portions of the BHCA and the Glass–Steagall Act, allowing banks, brokerages, and insurance companies to merge, thus making the CitiCorp/Travelers Group merger legal.

Also prior to the passage of the Act, there were many relaxations to the *Glass–Steagall Act*. For example, a few years earlier, commercial Banks were allowed to pursue investment banking, and before that banks were also allowed to begin stock and insurance brokerage. Insurance underwriting was the only main operation they weren't allowed to do, something rarely done by banks even after the passage of the Act. The Act further enacted three provisions that allow for bank holding companies to engage in physical commodity activities. Prior to the enactment of the Act those activities were limited to those that were so closely related to banking to be considered incidental to it. Under GLBA depending on the provision the institution falls into, bank holding companies can engage in physical commodity trading, energy tolling, energy management services, and merchant banking activities.[[21]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-26)

Much consolidation occurred in the financial services industry since, but not at the scale some had expected. Retail banks, for example, do not tend to buy insurance underwriters, as they seek to engage in a more profitable business of insurance brokerage by selling products of other insurance companies. Other retail banks were slow to market investments and insurance products and package those products in a convincing way. Brokerage companies had a hard time getting into banking, because they do not have a large branch and [backshop](https://en.wikipedia.org/wiki/Backshop) footprint. Banks have recently tended to buy other banks, such as the 2004 [Bank of America](https://en.wikipedia.org/wiki/Bank_of_America) and [Fleet Boston](https://en.wikipedia.org/wiki/Fleet_Boston) merger, yet they have had less success integrating with investment and insurance companies. Many banks have expanded into [investment banking](https://en.wikipedia.org/wiki/Investment_banking), but have found it hard to package it with their banking services, without resorting to questionable tie-ins which caused scandals at [Smith Barney](https://en.wikipedia.org/wiki/Smith_Barney).

Remaining restrictions[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=3)]

Crucial to the passing of this Act was an amendment made to the GLBA, stating that no merger may go ahead if any of the financial holding institutions, or affiliates thereof, received a "less than satisfactory [[*sic*](https://en.wikipedia.org/wiki/Sic)] rating at its most recent CRA exam", essentially meaning that any merger may only go ahead with the strict approval of the regulatory bodies responsible for the [Community Reinvestment Act](https://en.wikipedia.org/wiki/Community_Reinvestment_Act) (CRA).[[22]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-Community_Reinvestment_Act_Amendments_in_the_Gramm%E2%80%93Leach_Act-27) This was an issue of hot contention, and the Clinton Administration stressed that it "would veto any legislation that would scale back minority-lending requirements."[[23]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-Compromise_over_Community_Reinvestment_Act_crucial_to_repeal_of_Glass-Steagall-28)

GLBA also did not remove the restrictions on banks placed by the [Bank Holding Company Act of 1956](https://en.wikipedia.org/wiki/Bank_Holding_Company_Act_of_1956) which prevented financial institutions from owning non-financial corporations. It conversely prohibits corporations outside of the banking or finance industry from entering retail and/or commercial banking. Many assume [Wal-Mart](https://en.wikipedia.org/wiki/Wal-Mart)'s desire to convert its industrial bank to a commercial/retail bank ultimately drove the banking industry to back the GLBA restrictions.

Some restrictions remain to provide some amount of separation between the investment and commercial banking operations of a company. For example, [licensed](https://en.wikipedia.org/wiki/General_Securities_Representative_Exam) bankers must have separate business cards, e.g., "Personal Banker, Wells Fargo Bank" and "Investment Consultant, Wells Fargo Private Client Services". Much of the debate about [financial privacy](https://en.wikipedia.org/wiki/Financial_privacy) is specifically centered around allowing or preventing the banking, brokerage, and insurances divisions of a company from working together.

In terms of [compliance](https://en.wikipedia.org/wiki/Compliance_(regulation)), the key rules under the Act include *The Financial Privacy Rule* which governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, regardless of whether they are financial institutions, that receive such information. *The Safeguards Rule* requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions – such as credit reporting agencies, appraisers, and mortgage brokers – that receive customer information from other financial institutions.

Privacy[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=4)]

* GLBA compliance is mandatory; whether a financial institution discloses nonpublic information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity.
* Major components put into place to govern the collection, disclosure, and protection of consumers' nonpublic personal information; or personally identifiable information include:
  + [Financial Privacy Rule](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Financial_Privacy_Rule)
  + [Safeguards Rule](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Safeguards_Rule)
  + [Pretexting Protection](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#Pretexting_protection)

Financial Privacy Rule[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=5)]

(Subtitle A: Disclosure of Nonpublic Personal Information, codified at [15 U.S.C.](https://en.wikipedia.org/wiki/Title_15_of_the_United_States_Code) [§§ 6801](https://www.law.cornell.edu/uscode/text/15/6801)–[6809](https://www.law.cornell.edu/uscode/text/15/6809))

The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected. The notice must also identify the consumer's right to opt out of the information being shared with unaffiliated parties pursuant to the provisions of the [Fair Credit Reporting Act](https://en.wikipedia.org/wiki/Fair_Credit_Reporting_Act). Should the privacy policy change at any point in time, the consumer must be notified again for acceptance. Each time the privacy notice is reestablished, the consumer has the right to opt out again. The unaffiliated parties receiving the nonpublic information are held to the acceptance terms of the consumer under the original relationship agreement. In summary, the financial privacy rule provides for a [privacy policy](https://en.wikipedia.org/wiki/Privacy_policy) agreement between the company and the consumer pertaining to the protection of the consumer's personal nonpublic information.

On November 17, 2009, eight federal regulatory agencies released the final version of a [model privacy notice form](https://www.sec.gov/news/press/2009/2009-248.htm) to make it easier for consumers to understand how financial institutions collect and share information about consumers.

**Financial institutions**[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=6)]

GLBA defines financial institutions as: "companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance". The [Federal Trade Commission](https://en.wikipedia.org/wiki/Federal_Trade_Commission) (FTC) has jurisdiction over financial institutions similar to, and including, these:

* Non-bank mortgage lenders,
* Real estate appraisers,
* Loan brokers,
* Some financial or investment advisers,
* Debt collectors,
* Tax return preparers,
* Banks, and
* Real estate settlement service providers.

These companies must also be considered significantly engaged in the financial service or production that defines them as a "financial institution".

Insurance has jurisdiction first by the state, provided the state law at minimum complies with the GLB. State law can require greater compliance, but not less than what is otherwise required by the GLB.

**Consumer vs. customer defined**[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=7)]

The *Gramm–Leach–Bliley Act* defines a "consumer" as

"an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." (See [15 U.S.C.](https://en.wikipedia.org/wiki/Title_15_of_the_United_States_Code) [§ 6809(9)](https://www.law.cornell.edu/uscode/text/15/6809(9)).)

A customer is a consumer that has developed a relationship with privacy rights protected under the *GLB*. A customer is not someone using an automated teller machine (ATM) or having a check cashed at a cash advance business. These are not ongoing relationships like a customer might have—i.e., a [mortgage loan](https://en.wikipedia.org/wiki/Mortgage_loan), tax advising, or credit financing. A business is not an individual with personal nonpublic information, so a business cannot be a customer under the *GLB*. A business, however, may be liable for compliance to the *GLB* depending upon the type of business and the activities utilizing individual's personal nonpublic information.

Definition: A "consumer" is an individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

Examples of consumer relationships:

* Applying for a loan
* Obtaining cash from a foreign ATM, even if it occurs on a regular basis
* Cashing a check with a check-cashing company
* Arranging for a wire transfer[[24]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-ftcoutline-29)

Definition: A "customer" is a consumer who has a "customer relationship" with a financial institution. A "customer relationship" is a continuing relationship with a consumer.

Examples of establishing a customer relationship:

* Opening a credit card account with a financial institution
* Entering into an automobile lease (on a non-operating basis for an initial lease term of at least 90 days) with an automobile dealer
* Providing personally identifiable financial information to a broker in order to obtain a mortgage loan
* Obtaining a loan from a mortgage lender
* Agreeing to obtain tax preparation or credit counseling services

"Special Rule" for Loans: The customer relationship travels with ownership of the servicing rights.[[24]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-ftcoutline-29)

**Consumer/client privacy rights**[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=8)]

Under the *GLB*, financial institutions must provide their clients a privacy notice that explains what information the company gathers about the client, where this information is shared, and how the company safeguards that information. This privacy notice must be given to the client prior to entering into an agreement to do business. There are exceptions to this when the client accepts a delayed receipt of the notice in order to complete a transaction on a timely basis. This has been somewhat mitigated due to online acknowledgement agreements requiring the client to read or scroll through the notice and check a box to accept terms.

The privacy notice must also explain to the customer the opportunity to 'opt out'. Opting out means that the client can say "no" to allowing their information to be shared with nonaffiliated third parties. The [*Fair Credit Reporting Act*](https://en.wikipedia.org/wiki/Fair_Credit_Reporting_Act) is responsible for the 'opt-out' opportunity, but the privacy notice must inform the customer of this right under the GLB. The client cannot opt out of:

* Information shared with those providing priority service to the financial institution
* Marketing of products or services for the financial institution
* When the information is deemed legally required.
* When entering into a financial transaction, the institution providing said transaction must provide the customer a secure room with the ability to close in order to better protect the clients personal information.

Receipt of GLBA notices by consumers[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=9)]

**Service of notice requirements**[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=10)]

Notice requirements may vary. In most cases, service of a GLBA notice is not necessary unless the entity serving the notice intends to "share" customer information, which the FTC defines as, "non-public personal information (NPI)", of customers required to be protected under *GLBA*.[[25]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-30)[[26]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-31)[[27]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-32)

**Response to receipt of a GLBA notice**[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=11)]

A consumer may respond to service of a *GLBA* notice by:

* No response
* Indicating, on an acknowledgment form that notice was not provided (typically for in-person signed documents)
* Responding according to format suggested in the GLBA Notice
* Responding with a prepared letter (alone or in addition to the form)

Synergy between GLBA and GDPR[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=12)]

The [European Union's](https://en.wikipedia.org/wiki/European_Union) [General Data Protection Regulation (GDPR)](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation) became enforceable on 25 May 2018. As applies to consumers, the [GDPR](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation) includes provision on scope of data collection, but also includes [right of access](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation#Right_of_access), [right to erasure](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation#Right_to_erasure), right to restriction of processing and right to data portability. Due to the multinational nature of some transactions, including data and internet transactions, and the possible implementation of corresponding regulations in some US states, it is likely that business and other entities will comply with the [GDPR](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation) as well as US *GLBA* requirements.

Individualized requests for privacy under the *GLBA* are likely to include provisions guaranteed by the [European Union](https://en.wikipedia.org/wiki/European_Union)'s [GDPR](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation).

Safeguards Rule[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=13)]

(Subtitle A: Disclosure of Nonpublic Personal Information, codified at [15 U.S.C.](https://en.wikipedia.org/wiki/Title_15_of_the_United_States_Code) [§§ 6801](https://www.law.cornell.edu/uscode/text/15/6801)–[6809](https://www.law.cornell.edu/uscode/text/15/6809))

The Safeguards Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. (The Safeguards Rule applies to information of any consumers past or present of the financial institution's products or services.) This plan must include:

* Denoting at least one employee to manage the safeguards,
* Constructing a thorough [risk analysis](https://en.wikipedia.org/wiki/Risk_analysis_(business)) on each department handling the nonpublic information,
* Develop, monitor, and test a program to secure the information, and
* Change the safeguards as needed with the changes in how information is collected, stored, and used.

The Safeguards Rule forces financial institutions to take a closer look at how they manage private data and to do a risk analysis on their current processes. No process is perfect, so this has meant that every financial institution has had to make some effort to comply with the *GLBA*.

Pretexting protection[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=14)]

(Subtitle B: Fraudulent Access to Financial Information, codified at [15 U.S.C.](https://en.wikipedia.org/wiki/Title_15_of_the_United_States_Code) [§§ 6821](https://www.law.cornell.edu/uscode/text/15/6821)–[6827](https://www.law.cornell.edu/uscode/text/15/6827))

[Pretexting](https://en.wikipedia.org/wiki/Pretexting) (sometimes referred to as "social engineering") occurs when someone tries to gain access to personal nonpublic information without proper authority to do so. This may entail requesting private information while impersonating the account holder, by phone, by mail, by email, or even by "[phishing](https://en.wikipedia.org/wiki/Phishing)" (i.e., using a phony website or email to collect data). GLBA encourages the organizations covered by GLBA to implement safeguards against pretexting. For example, a well-written plan designed to meet GLB's Safeguards Rule ("develop, monitor, and test a program to secure the information") would likely include a section on training employees to recognize and deflect inquiries made under pretext. In fact, the evaluation of the effectiveness of such employee training probably should include a follow-up program of random spot checks, "outside the classroom", after completion of the [initial] employee training, in order to check on the resistance of a given (randomly chosen) student to various types of "social engineering"—perhaps even designed to focus attention on any new wrinkle that might have arisen *after* the [initial] effort to "develop" the curriculum for such employee training. Under United States law, pretexting by individuals is punishable as a [common law](https://en.wikipedia.org/wiki/Common_law) crime of [false pretenses](https://en.wikipedia.org/wiki/False_pretenses).

Effect on usury law[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=15)]

Section 731 of the GLB, codified as subsection (f) of [12 U.S.C.](https://en.wikipedia.org/wiki/Title_12_of_the_United_States_Code) [§ 1831u](https://www.law.cornell.edu/uscode/text/12/1831u), contains a unique provision aimed at [Arkansas](https://en.wikipedia.org/wiki/Arkansas), whose [usury](https://en.wikipedia.org/wiki/Usury) limit was set at five percent above the [Federal Reserve discount rate](https://en.wikipedia.org/wiki/Discount_window) by the [Arkansas Constitution](https://en.wikipedia.org/wiki/Arkansas_Constitution) and could not be changed by the [Arkansas General Assembly](https://en.wikipedia.org/wiki/Arkansas_General_Assembly). When the [Office of the Comptroller of the Currency](https://en.wikipedia.org/wiki/Office_of_the_Comptroller_of_the_Currency) ruled that interstate banks established under the [Riegle-Neal Interstate Banking and Branching Efficiency Act of 1994](https://en.wikipedia.org/wiki/Riegle-Neal_Interstate_Banking_and_Branching_Efficiency_Act_of_1994) could use their home state's usury law for all branches nationwide with minimal restrictions,[[28]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-33) Arkansas-based banks were placed at a severe competitive disadvantage to Arkansas branches of interstate banks; this led to out-of-state takeovers of several Arkansas banks, including the sale of First Commercial Bank (then Arkansas' largest bank) to [Regions Financial Corporation](https://en.wikipedia.org/wiki/Regions_Financial_Corporation) in 1998.

Under Section 731, all banks headquartered in a state covered by that law may charge up to the highest usury limit of any state that is headquarters to an interstate bank which has branches in the covered state. Therefore, since Arkansas has branches of banks based in [Alabama](https://en.wikipedia.org/wiki/Alabama), [Georgia](https://en.wikipedia.org/wiki/Georgia_(U.S._state)), [Mississippi](https://en.wikipedia.org/wiki/Mississippi), [Missouri](https://en.wikipedia.org/wiki/Missouri), [North Carolina](https://en.wikipedia.org/wiki/North_Carolina), [Ohio](https://en.wikipedia.org/wiki/Ohio), and [Texas](https://en.wikipedia.org/wiki/Texas),[[29]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-34) any loan that is legal under the usury laws of any of those states may be made by an Arkansas-based bank under Section 731. The section does not apply to interstate banks with branches in the covered state, but headquartered elsewhere; however, Arkansas-based interstate banks like [Arvest Bank](https://en.wikipedia.org/wiki/Arvest_Bank) may export their Section 731 limits to other states.

Due to Section 731, it is generally regarded that Arkansas-based banks now have no usury limit for [credit cards](https://en.wikipedia.org/wiki/Credit_card) or for any loan of greater than $2,000 (since Alabama, Regions' home state, has no limits on those loans), with a limit of 18% (the minimum usury limit in Texas) or more on all other loans.[[30]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-35) However, once [Wells Fargo](https://en.wikipedia.org/wiki/Wells_Fargo) fully completed its purchase of Century Bank (a Texas bank with Arkansas branches), Section 731 did away with all usury limits for Arkansas-based banks since Wells Fargo's main bank charter is based in [South Dakota](https://en.wikipedia.org/wiki/South_Dakota), which repealed its usury laws many years ago.

Though designed for Arkansas, Section 731 may also apply to [Alaska](https://en.wikipedia.org/wiki/Alaska) and [California](https://en.wikipedia.org/wiki/California) whose constitutions provide for the same basic usury limit, though unlike Arkansas their legislatures can (and generally do) set different limits. If Section 731 applies to those states, then all their usury limits are inapplicable to banks based in those states, since Wells Fargo has branches in both states.

Controversy[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=16)]

*See also:*[*Subprime mortgage crisis § Causes*](https://en.wikipedia.org/wiki/Subprime_mortgage_crisis#Causes)

**Criticisms**[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=17)]

The act is often cited as a cause of the [2007 subprime mortgage financial crisis](https://en.wikipedia.org/wiki/2007_subprime_mortgage_financial_crisis) "even by some of its onetime supporters."[[31]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-36) Former President Barack Obama has stated that GLBA led to deregulation that, among other things, allowed for the creation of giant financial supermarkets that could own investment banks, commercial banks and insurance firms, something banned since the Great Depression. Its passage, critics also say, cleared the way for companies that were [too big and intertwined to fail](https://en.wikipedia.org/wiki/Too_big_to_fail).[[32]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-37)

[Nobel Prize](https://en.wikipedia.org/wiki/Nobel_Memorial_Prize_in_Economic_Sciences)-winning economist [Joseph Stiglitz](https://en.wikipedia.org/wiki/Joseph_Stiglitz) has also argued that the Act helped to create the crisis.[[33]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-38) In an article in [*The Nation*](https://en.wikipedia.org/wiki/The_Nation), Mark Sumner asserted that the Gramm–Leach–Bliley Act was responsible for the creation of entities that took on more risk due to their being considered "[too big to fail](https://en.wikipedia.org/wiki/Too_big_to_fail)".[[34]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-39)

According to a 2009 policy report from the [Cato Institute](https://en.wikipedia.org/wiki/Cato_Institute) authored by one of the institute's directors, [Mark A. Calabria](https://en.wikipedia.org/wiki/Mark_A._Calabria), critics of the legislation feared that, with the allowance for mergers between investment and commercial banks, GLBA allowed the newly-merged banks to take on riskier investments while at the same time removing any requirements to maintain enough equity, exposing the assets of its banking customers.[[35]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-Calabria-40)[[*non-primary source needed*](https://en.wikipedia.org/wiki/Wikipedia:No_original_research#Primary,_secondary_and_tertiary_sources)] Calabria claimed that, prior to the passage of GLBA in 1999, investment banks were already capable of holding and trading the very financial assets claimed to be the cause of the mortgage crisis, and were also already able to keep their books as they had.[[35]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-Calabria-40) He concluded that greater access to investment capital as many investment banks went public on the market explains the shift in their holdings to trading portfolios.[[35]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-Calabria-40) Calabria noted that after GLBA passed, most investment banks did not merge with depository commercial banks, and that in fact, the few banks that did merge weathered the crisis better than those that did not.[[35]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-Calabria-40)

In February 2009, one of the act's co-authors, former Senator Phil Gramm, also defended his bill:

[I]f GLB was the problem, the crisis would have been expected to have originated in Europe where they never had Glass–Steagall requirements to begin with. Also, the financial firms that failed in this crisis, like [Lehman](https://en.wikipedia.org/wiki/Lehman_Brothers), were the least diversified and the ones that survived, like [J.P. Morgan](https://en.wikipedia.org/wiki/JPMorgan_Chase), were the most diversified. Moreover, GLB did not deregulate anything. It established the Federal Reserve as a superregulator, overseeing all Financial Services Holding Companies. All activities of financial institutions continued to be regulated on a functional basis by the regulators that had regulated those activities prior to GLB.[[36]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-41)

[Bill Clinton](https://en.wikipedia.org/wiki/Bill_Clinton), as well as economists [Brad DeLong](https://en.wikipedia.org/wiki/Brad_DeLong) and [Tyler Cowen](https://en.wikipedia.org/wiki/Tyler_Cowen) have all argued that the Gramm–Leach–Bliley Act softened the impact of the crisis.[[37]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-42)[[38]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-43) [*Atlantic Monthly*](https://en.wikipedia.org/wiki/Atlantic_Monthly) columnist [Megan McArdle](https://en.wikipedia.org/wiki/Megan_McArdle) has argued that if the act was "part of the problem, it would be the commercial banks, not the investment banks, that were in trouble" and repeal would not have helped the situation.[[39]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-44) An article in the [conservative](https://en.wikipedia.org/wiki/Conservativism_in_the_United_States) publication [*National Review*](https://en.wikipedia.org/wiki/National_Review) has made the same argument, calling allegations about the Act "[folk economics](https://en.wikipedia.org/wiki/Folklore)."[[40]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-45) A [*New York Times*](https://en.wikipedia.org/wiki/New_York_Times) financial columnist and occasional critic of GLBA [Andrew Ross Sorkin](https://en.wikipedia.org/wiki/Andrew_Ross_Sorkin) stated that he believes GLBA had little to do with the failed institutions.[[41]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-46)

Amendments[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=18)]

**Proposed**[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=19)]

* [National Association of Registered Agents and Brokers Reform Act of 2013 (H.R. 1155; 113th Congress)](https://en.wikipedia.org/wiki/National_Association_of_Registered_Agents_and_Brokers_Reform_Act_of_2013_(H.R._1155;_113th_Congress)) ([H.R. 1155](https://www.congress.gov/bill/113th-congress/house-bill/1155)) is a bill meant to reduce the regulatory costs of complying with multiple states' requirements for insurance companies, making it easier for the same company to operate in multiple states.[[42]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-Kasper1-47) The bill would amend the Gramm–Leach–Bliley Act to repeal the contingent conditions under which the National Association of Registered Agents and Brokers (NARAB) shall not be established.[[43]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-1155sum-48) The bill would transform the National Association of Registered Agents and Brokers (NARAB) into a clearing house that set up its own standards that insurance companies would be required to meet in order to do business in other states.[[42]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-Kasper1-47) In this new system, however, the insurance company would only have to meet the requirements of their home state and the NARAB (only two entities), not their home state and every other state they wished to operate in (multiple entities).[[42]](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act#cite_note-Kasper1-47) Proponents of the bill argued that it would help lower costs for insurance companies and make insurance cheaper for people to buy.

See also[[edit](https://en.wikipedia.org/w/index.php?title=Gramm%E2%80%93Leach%E2%80%93Bliley_Act&action=edit&section=20)]

* [Bank regulation](https://en.wikipedia.org/wiki/Bank_regulation)
* [Securities regulation in the United States](https://en.wikipedia.org/wiki/Securities_regulation_in_the_United_States)
* [Commodity Futures Trading Commission](https://en.wikipedia.org/wiki/Commodity_Futures_Trading_Commission)
* [Securities commission](https://en.wikipedia.org/wiki/Securities_commission)
* [Chicago Stock Exchange](https://en.wikipedia.org/wiki/Chicago_Stock_Exchange)
* [Financial regulation](https://en.wikipedia.org/wiki/Financial_regulation)
* [Financial privacy laws in the United States](https://en.wikipedia.org/wiki/Financial_privacy_laws_in_the_United_States)
* [*Inside Job*](https://en.wikipedia.org/wiki/Inside_Job_(2010_film)) (2010 documentary film)
* [List of financial regulatory authorities by country](https://en.wikipedia.org/wiki/List_of_financial_regulatory_authorities_by_country)
* [NASDAQ](https://en.wikipedia.org/wiki/NASDAQ)
* [New York Stock Exchange](https://en.wikipedia.org/wiki/New_York_Stock_Exchange)
* [Stock exchange](https://en.wikipedia.org/wiki/Stock_exchange)
* [Regulation D (SEC)](https://en.wikipedia.org/wiki/Regulation_D_(SEC))

**Related legislation**

* 1933 – [Securities Act of 1933](https://en.wikipedia.org/wiki/Securities_Act_of_1933)
* 1933 – [Banking Act of 1933](https://en.wikipedia.org/wiki/1933_Banking_Act), which contained legislation repealed by Gramm–Leach–Bliley
* 1934 – [Securities Exchange Act of 1934](https://en.wikipedia.org/wiki/Securities_Exchange_Act_of_1934)
* 1938 – [Temporary National Economic Committee](https://en.wikipedia.org/wiki/Temporary_National_Economic_Committee) (establishment)
* 1939 – [Trust Indenture Act of 1939](https://en.wikipedia.org/wiki/Trust_Indenture_Act_of_1939)
* 1940 – [Investment Advisers Act of 1940](https://en.wikipedia.org/wiki/Investment_Advisers_Act_of_1940)
* 1940 – [Investment Company Act of 1940](https://en.wikipedia.org/wiki/Investment_Company_Act_of_1940)
* 1968 – [Williams Act](https://en.wikipedia.org/wiki/Williams_Act) (Securities Disclosure Act)
* 1975 – [Securities and Exchange Act](https://en.wikipedia.org/wiki/Securities_and_Exchange_Act)
* 1982 – [Garn–St. Germain Depository Institutions Act](https://en.wikipedia.org/wiki/Garn%E2%80%93St._Germain_Depository_Institutions_Act)
* 2000 – [Commodity Futures Modernization Act of 2000](https://en.wikipedia.org/wiki/Commodity_Futures_Modernization_Act_of_2000)
* 2002 – [Sarbanes–Oxley Act](https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act)
* 2003 – [Fair and Accurate Credit Transactions Act](https://en.wikipedia.org/wiki/Fair_and_Accurate_Credit_Transactions_Act) of 2003
* 2006 – [Credit Rating Agency Reform Act](https://en.wikipedia.org/wiki/Credit_Rating_Agency_Reform_Act) of 2006
* 2010 – [Dodd–Frank Wall Street Reform and Consumer Protection Act](https://en.wikipedia.org/wiki/Dodd%E2%80%93Frank_Wall_Street_Reform_and_Consumer_Protection_Act)

About FINRA Industry Financial

Financial Industry Regulatory Authority

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#p-search)

|  |  |  |  |
| --- | --- | --- | --- |
|  | hide**This article has multiple issues.** Please help [**improve it**](https://en.wikipedia.org/w/index.php?title=Financial_Industry_Regulatory_Authority&action=edit) or discuss these issues on the [**talk page**](https://en.wikipedia.org/wiki/Talk:Financial_Industry_Regulatory_Authority). *(*[*Learn how and when to remove these template messages*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)*   |  | | --- | | This article **reads like**[**a press release**](https://en.wikipedia.org/wiki/Wikipedia:What_Wikipedia_is_not#SOAPBOX)**or**[**a news article**](https://en.wikipedia.org/wiki/Wikipedia:What_Wikipedia_is_not#NEWS) or **is largely based on**[**routine coverage**](https://en.wikipedia.org/wiki/Wikipedia:Notability_(events)#Routine_coverage) or [**sensationalism**](https://en.wikipedia.org/wiki/Wikipedia:Notability_(events)#Sensationalism). *(March 2013)* |  |  | | --- | | This article **has been nominated to be checked for its**[**neutrality**](https://en.wikipedia.org/wiki/Wikipedia:Neutral_point_of_view). *(March 2013)* | |

|  |  |
| --- | --- |
| **Financial Industry Regulatory Authority** | |
| **Founded** | July 30, 2007[[1]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-1) |
| **Headquarters** | [Washington, D.C.](https://en.wikipedia.org/wiki/Washington,_D.C.) |
| **Key people** | Robert W. Cook, president and chief executive officer |
| **Employees** | 3,600[[2]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-finra.org-2) |
| **Website** | [www.finra.org](http://www.finra.org/) |

In the [United States](https://en.wikipedia.org/wiki/United_States), the **Financial Industry Regulatory Authority, Inc.** (**FINRA**) is a private corporation that acts as a [self-regulatory organization](https://en.wikipedia.org/wiki/Self-regulatory_organization) (SRO). FINRA is the successor to the **National Association of Securities Dealers, Inc.** (**NASD**) and the member regulation, enforcement, and arbitration operations of the [New York Stock Exchange](https://en.wikipedia.org/wiki/New_York_Stock_Exchange). It is a non-governmental organization that [regulates](https://en.wikipedia.org/wiki/Financial_regulation) member [brokerage firms](https://en.wikipedia.org/wiki/Brokerage_firm) and [exchange markets](https://en.wikipedia.org/wiki/Exchange_(organized_market)). The government agency which acts as the ultimate regulator of the securities industry, including FINRA, is the [Securities and Exchange Commission](https://en.wikipedia.org/wiki/U.S._Securities_and_Exchange_Commission).



**Contents**

* [1Overview](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#Overview)
* [2History](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#History)
* [3Board of governors](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#Board_of_governors)
* [4Functions: regulation and licensure](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#Functions:_regulation_and_licensure)
* [5Central Registration Depository](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#Central_Registration_Depository)
* [6Size](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#Size)
* [7Criticism](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#Criticism)
* [8Arbitration](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#Arbitration)
* [9See also](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#See_also)
* [10References](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#References)
* [11External links](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#External_links)

Overview[[edit](https://en.wikipedia.org/w/index.php?title=Financial_Industry_Regulatory_Authority&action=edit&section=1)]

The Financial Industry Regulatory Authority is the largest independent regulator for all securities firms doing business in the United States. FINRA's mission is to protect investors by making sure the United States securities industry operates fairly and honestly. FINRA oversees about 4,250 brokerage firms, about 162,155 branch offices and approximately 629,525 registered securities representatives.[[2]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-finra.org-2)[[3]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-3)

FINRA has approximately 3,400 employees and operates from Washington, D.C. and New York, NY, with 20 regional offices around the country.[[2]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-finra.org-2)

FINRA offers regulatory oversight over all securities firms that do business with the public, plus those offering professional training, testing, and licensing of registered persons, arbitration and mediation, market regulation by contract for the [New York Stock Exchange](https://en.wikipedia.org/wiki/New_York_Stock_Exchange), the [NASDAQ](https://en.wikipedia.org/wiki/NASDAQ) Stock Market, Inc., the [American Stock Exchange](https://en.wikipedia.org/wiki/American_Stock_Exchange) LLC, and the [International Securities Exchange](https://en.wikipedia.org/wiki/International_Securities_Exchange), LLC; and industry utilities, such as Trade Reporting Facilities and other over-the-counter operations.

FINRA was formed by a consolidation of the member regulation, enforcement, and arbitration operations of the [New York Stock Exchange](https://en.wikipedia.org/wiki/New_York_Stock_Exchange), NYSE Regulation, Inc., and NASD. The merger was approved by the United States [Securities and Exchange Commission](https://en.wikipedia.org/wiki/Securities_and_Exchange_Commission) (SEC) on July 26, 2007.[[4]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-4)

History[[edit](https://en.wikipedia.org/w/index.php?title=Financial_Industry_Regulatory_Authority&action=edit&section=2)]

The NASD was founded in 1939 and was registered with the SEC in response to the [1938 Maloney Act amendments](https://en.wikipedia.org/wiki/Securities_Exchange_Act_of_1934#Self-regulatory_organizations_.28SRO.29) to the [Securities Exchange Act of 1934](https://en.wikipedia.org/wiki/Securities_Exchange_Act_of_1934), which allowed it to supervise the conduct of its members subject to the oversight of the SEC. In 1971, NASD launched a new computerized stock trading system called the National Association of Securities Dealers Automated Quotations ([NASDAQ](https://en.wikipedia.org/wiki/NASDAQ)) stock market. The NYSE and [AMEX](https://en.wikipedia.org/wiki/American_Stock_Exchange) stock exchanges merged in 1998. Two years later, the NASDAQ underwent a major recapitalization and became an independent entity from NASD. In July 2007, the SEC approved the formation of a new SRO to be a successor to NASD. The NASD and the member regulation, enforcement and arbitration functions of the New York Stock Exchange were then consolidated into the Financial Industry Regulatory Authority (FINRA).[[5]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-5)

Board of governors[[edit](https://en.wikipedia.org/w/index.php?title=Financial_Industry_Regulatory_Authority&action=edit&section=3)]

The FINRA By-Laws provide that the FINRA Board must consist of the chief executive officer of FINRA, the chief executive officer of NYSE Regulation, eleven public governors, and ten industry governors, including a floor member governor, an independent dealer/insurance affiliate governor, an investment company affiliate governor, three small firm governors, one mid-size firm governor, and three large-firm governors. The small firm governors, mid-size firm governor, and large-firm governors are elected by members of FINRA according to their classification as a small firm, mid-size firm, or large firm.[[6]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-6)[[7]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-7)

Functions: regulation and licensure[[edit](https://en.wikipedia.org/w/index.php?title=Financial_Industry_Regulatory_Authority&action=edit&section=4)]

FINRA regulates trading in equities, corporate bonds, securities futures, and options. All firms dealing in securities that are not regulated by another SRO, such as by the [Municipal Securities Rulemaking Board](https://en.wikipedia.org/wiki/Municipal_Securities_Rulemaking_Board) (MSRB), are required to be member firms of the FINRA.

As part of its regulatory authority, FINRA periodically conducts regulatory exams of its regulated institutions. FINRA recently released its tenth annual Regulatory and Examinations Priorities Letter for 2015, which impacts broker-dealers as well as their affiliated insurance companies and banks. In its Regulatory and Examinations Priorities Letter for 2015 FINRA has identified variable annuities as a significant area of focus for exams in 2015 and has pointed out particular elements of sales practices that will be reviewed.[[8]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-8)

FINRA licenses individuals and admits firms to the industry, writes rules to govern their behavior, examines them for regulatory compliance, and is sanctioned by the U.S. Securities and Exchange Commission (SEC) to discipline registered representatives and member firms that fail to comply with federal securities laws and FINRA's rules and regulations. It provides education and qualification examinations to industry professionals. It also sells outsourced regulatory products and services to a number of stock markets and exchanges; e.g. [American Stock Exchange](https://en.wikipedia.org/wiki/American_Stock_Exchange) (AMEX) and the [International Securities Exchange](https://en.wikipedia.org/wiki/International_Securities_Exchange) (ISE).

NASD, the predecessor of FINRA, founded the [NASDAQ](https://en.wikipedia.org/wiki/NASDAQ) ("National Association of Securities Dealers Automated Quotations") stock market in 1971. In 2006, NASD demutualized from NASDAQ by selling its ownership interest.

The NASD, now FINRA, publishes much educational information for the public and has been publishing and disclosing the education and exam requirements for USA based credentials, charters, designations and certifications that are offered by [SROs](https://en.wikipedia.org/wiki/Self-regulatory_organization) for about a decade.[[9]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-9)

Central Registration Depository[[edit](https://en.wikipedia.org/w/index.php?title=Financial_Industry_Regulatory_Authority&action=edit&section=5)]

On behalf of state securities regulators, FINRA maintains the Central Registration Depository (CRD), the central database containing records for all firms and individuals involved in the securities industry in the United States.[[10]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-10)

Size[[edit](https://en.wikipedia.org/w/index.php?title=Financial_Industry_Regulatory_Authority&action=edit&section=6)]

FINRA had total revenues of US$878.6 million in 2012.[[2]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-finra.org-2)[[11]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-11) FINRA is funded primarily by assessments of member firms' registered representatives and applicants, annual fees paid by members, and by fines that it levies. The annual fee that each member pays includes a basic membership fee, an assessment based on gross income, a fee for each principal and registered representative, and charge for each branch office.

Criticism[[edit](https://en.wikipedia.org/w/index.php?title=Financial_Industry_Regulatory_Authority&action=edit&section=7)]

According to a study by Deborah G. Heilizer and Brian L. Rubin, partners at the Washington, D.C. law firm [Sutherland Asbill & Brennan LLP](https://en.wikipedia.org/wiki/Sutherland_Asbill_%26_Brennan_LLP), regulators with NASD and NYSE Regulation (now collectively known as FINRA) obtained supersized fines (i.e., fines over US$1 million) in 35 actions taken in 2005. In 2006, however, that number dropped to 19; furthermore, the number of enforcement actions over US$5 million also fell. In 2005, there were seven such actions as opposed to three in 2006. According to the written report, the "data suggest that securities regulators may have retrenched their efforts to regulate through the use of novel theories."[[12]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-12)

FINRA collected fines against financial firms totaling US$25.9 million in 2008, a third straight annual decline in fines levied by FINRA or one of its predecessor agencies. The 2008 total was 82% below the US$148.5 million in fines collected in 2005. According to FINRA, the fines levied in 2009 were 47.6 million, declining slightly to $42.2 million in 2010 and then expanding to $71.9 million for 2011.[[13]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-13)

Arbitration[[edit](https://en.wikipedia.org/w/index.php?title=Financial_Industry_Regulatory_Authority&action=edit&section=8)]

FINRA operates the largest arbitration forum in the United States for the resolution of disputes between customers and member firms, as well as between brokerage firm employees and their firms. (This function had been performed by both NASD and NYSE's regulation committee until their merger in 2007 to form FINRA. Each entity had its own set of rules on arbitration procedures. After its creation, FINRA Dispute Resolution harmonized the prior NYSE and NASD rules.[[14]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-14)) Virtually all agreements between investors and their stockbrokers include mandatory arbitration agreements, whereby investors (and the brokerage firms) waive their right to trial in a court of law. While arbitration cases are the usual resolution procedure of last resort, class action cases are brought and often permitted to go forward in courts as well, where binding arbitration contracts are sometimes rejected, typically after being ruled unconscionable; see [*Wilko v. Swan*](https://en.wikipedia.org/wiki/Wilko_v._Swan). Although the fairness of such mandatory arbitration clauses has been called into question, U.S. courts have often found them to be lawful and have generally upheld both the enforceability and result of these arbitrations, except in the case of [class actions](https://en.wikipedia.org/wiki/Class_action).[[15]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-sbpllplaw.com-15)

As of May 2011, the pool of arbitrators consisted of 2,854 individuals classified by FINRA as industry panelists and 3,557 individuals classified as non-industry panelists.[[16]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-FINRA_STATS-16)

In 1987, the [United States Supreme Court](https://en.wikipedia.org/wiki/United_States_Supreme_Court) ruled in [*Shearson/American Express Inc. v. McMahon*](https://en.wikipedia.org/wiki/Shearson/American_Express_Inc._v._McMahon) that clauses mandating [arbitration](https://en.wikipedia.org/wiki/Arbitration_in_the_United_States) for disputes under the [Securities Exchange Act of 1934](https://en.wikipedia.org/wiki/Securities_Exchange_Act_of_1934) were enforceable. Three years later, it overturned *Wilko* completely in [*Rodriguez de Quijas v. Shearson/American Express Inc.*](https://en.wikipedia.org/wiki/Rodriguez_de_Quijas_v._Shearson/American_Express_Inc.), extending the arbitration requirement to disputes under the [Securities Act of 1933](https://en.wikipedia.org/wiki/Securities_Act_of_1933). Thus, many securities disputes are now resolved in arbitration.

For disputes over $100,000 between customers and member firms, the panel that decides the case generally consists of three arbitrators: one industry (or, at the customer's timely discretion non-industry) panelist, one non-industry panelist, and one non-industry chairperson, according to the Code of Arbitration Procedure for Customer Disputes.[[17]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-17) For disputes between an employee and member firms, all three arbitrators are industry panelists, according to [the industry code](http://finra.complinet.com/en/display/display_viewall.html?rbid=2403&element_id=4193&record_id=5272). For a given case, the two sides are provided separate lists by FINRA of ten local arbitrators for each category from which each party can strike up to four arbitrators and provide a ranking for the rest. Also provided are ten-year biographies and prior award histories for each arbitrator. FINRA will then provide the parties with the panel members by selecting the highest ranked available arbitrator from each category.[[15]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-sbpllplaw.com-15)[[18]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-FINRA_RULES-18)

According to FINRA, there were 5,680 cases for arbitration filed in 2010, a decrease from the 7,137 cases filed in 2009. The percentage of cases in which customers are awarded damages has risen slightly from 42% in 2008 to 47–48% in 2010 and 2011.[[16]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-FINRA_STATS-16) FINRA rates any positive award to a customer as a win for the customer, regardless of the magnitude of losses or legal fees.[[19]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-NYT-06-2006-19)

FINRA rules do not require parties to be represented by attorneys. A party may also appear [*pro se*](https://en.wikipedia.org/wiki/Pro_se), or be represented by a non-attorney in arbitration. However, the third option is not advised since this may be the unauthorized practice of law.[[20]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-20) Brokerage firms routinely hire attorneys, so a customer who does not can be at a serious disadvantage. One organization whose members specialize in representing customers against brokerage firms in FINRA arbitrations is the [Public Investors Arbitration Bar Association](http://www.piaba.org/) (PIABA).

In June 2006, [Lewis D. Lowenfels](http://www.tolinslowenfels.com/LDL.html), one of two partners at the New York law firm of [Tolins & Lowenfels](http://www.tolinslowenfels.com/index.html) and co-author of the looseleaf treatise [Bromberg and Lowenfels on Securities Fraud and Commodities Fraud, 2d](https://web.archive.org/web/20071214184816/http:/west.thomson.com/store/product.aspx?product_id=13517027) said of the NASD arbitration process: "What started out as a relatively swift and economical process for a public customer claimant to seek justice has evolved into a costly extended adversarial proceeding dominated by trial lawyers and the usual litigation tactics."[[19]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-NYT-06-2006-19)

Perhaps amidst speculation that Congress was contemplating passing legislation[[21]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-FEINGOLD-21) preventing mandatory arbitration clauses, FINRA announced in July 2008 that it would be launching a pilot program to evaluate all-public arbitration panels (thus not requiring an industry arbitrator to be on each panel).[[22]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-FINRA_07-24-08-22) In February 2011, FINRA announced that it would be making the program permanent. In that announcement, Richard Ketchum, FINRA Chairman and Chief Executive Officer stated "We believe that giving investors the ability to have an all-public panel will increase public confidence in the fairness of our dispute resolution process."[[23]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-FINRA_02-01-11-23) There are those, however, who see valid reasons for including an industry arbitrator on each panel. According to Richard Jackson, a principal at the advisor firm of Schlindwein Associates, LLC "It's probably pretty important to have someone on the panel who has specific industry knowledge and past experience in that field to explain some of the complexities that may be at issue,"[[24]](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority#cite_note-24)

FINRA does have a broker check system. This system lists the registered and licensed professionals. Those who have had complaints will also remain in the online system. Others who have passed exams, but have let their licenses retire, are not listed in the system if they had a clean record on their U-5.

See also[[edit](https://en.wikipedia.org/w/index.php?title=Financial_Industry_Regulatory_Authority&action=edit&section=9)]

* [Securities market participants (United States)](https://en.wikipedia.org/wiki/Securities_market_participants_(United_States))
* [Securities Investor Protection Corporation](https://en.wikipedia.org/wiki/Securities_Investor_Protection_Corporation) (SIPC)
* [Municipal Securities Rulemaking Board](https://en.wikipedia.org/wiki/Municipal_Securities_Rulemaking_Board) (MSRB)
* [Securities and Exchange Commission](https://en.wikipedia.org/wiki/Securities_and_Exchange_Commission) (SEC)
* [NASDAQ](https://en.wikipedia.org/wiki/NASDAQ)
* [List of finance topics](https://en.wikipedia.org/wiki/List_of_finance_topics)
* [American Academy of Financial Management](https://en.wikipedia.org/wiki/American_Academy_of_Financial_Management)
* [Alternative display facility](https://en.wikipedia.org/wiki/Alternative_display_facility)
* [ACT (Nasdaq)](https://en.wikipedia.org/wiki/ACT_(Nasdaq))
* [Securities regulation in the United States](https://en.wikipedia.org/wiki/Securities_regulation_in_the_United_States)
* [List of Securities Examinations](https://en.wikipedia.org/wiki/List_of_Securities_Examinations)