STEPS

a partnership with

AMERICA

Partnering with Americans to get America Back to Work in the COVID-19 era

STEPS
a partnership with
AMERICA

TABLE OF CONTENTS

BRIEF OVERVIEW AND EXPLANATION

EXPLANATION OF EACH OF THE STEPS

RESEARCH AND DETAILS BEHIND THE STEPS

STEPS
a partnership with
AMERICA

BRIEF EXPLANATION AND PROGRAM OVERVIEW

STEPS
a partnership with
AMERICA

To my fellow Americans:

As Americans we are facing great challenges and because of this a group of renowned security and safety professionals have come together to create a process that we hope will enable our great nation to get back to work again. The process of reuniting us with our normal process will be a daunting task but we believe with practical and safe adherence to processes that not only have been part of our daily work lives but are adjusted to the new norm we can make this a smooth transition. This process was created as a way to partner with our government and local agencies to become part of what we call the STEPS Partnership with America.

We know the STEPS necessary to create what is needed the most, which is trust. Confidence and trust, that's what's needed if you want people who have been listening to the daily, hourly, and minute by minute drone of war to courageously and enthusiastically leave the safety of their homes and return to work.

The STEPS program is all about creating confidence and trust between business owners and employees, and between small businesses and customers. It's about eliminating confusion, especially as it pertains to COVID-19, and returning to a healthy work environment and returning to consuming goods and services. We can't ask business owners to do more than they can do. We can only ask them to follow some easy guidelines and do the best they can do with what they have.

Thank you for your consideration and we would appreciate your support in getting everyone in this great community called America back to work.

God Bless America!

Mark R. Perkins

Mark R. Perkins
Chief Executive Officer
ESI Convergent, Inc.
mperkins@esiconvergent.com
517.285.5851: Direct Line
STEPSbacktowork.com

STEPS
a partnership with
AMERICA

Creating a partnership with Americans is all about taking the right S.T.E.P.S.

Partnering with Americans to get America Back to Work is not a slogan, but a process of building confidence and trust. STEPS is a "Partnership with America" to do everything that is necessary and feasible right now to ensure that the right STEPS are being taken to protect health, privacy, and wellbeing.

The greatest challenge is doing the right things now, and not allowing missteps and future mistakes to erode momentum in getting Americans back to work. With all the misinformation, negative perspectives, and social media influences, it is necessary to put forth a plan that substantially alleviates or eliminates any reasons not to go back to work. In this way, people who are skeptical and fearful of returning to work can be reassured that the right STEPS are being taken to assure their health, privacy, and wellbeing.

The partnership must be common sensical and easy to understand. The STEPS taken must be done consistently and visibly. Any facility that puts forth publicly the "STEPS" moniker, is letting Americans know that the five easy to understand steps that are applicable to their business or facility are in practice.

S **S**ocial Distancing Policy
- CDC defined and implemented
- Federal and State Guidelines

T **T**esting Guidelines for employees and visitors
- Government Medical Alliances
- Drug Testing Guidelines

E **E**ntry Assessment Program, (EAP)
- bSMART® Guidelines
- Security Consultants

P **P**rivacy Policy, (PP)
- Properly managing high risk individuals
- Existing Legal Precedent

S **S**tay Home / Work-From-Home, (WFH)
- Incentive Program
- Government/Private Partnership

STEP 1: Social Distancing

Social Distancing Policy has already been implemented across all States. The guidelines can be changed over time and having this be the first step in the Partnership with America creates a starting point that almost all Americans agree upon.

STEP 2: Testing Guidelines

Testing Guidelines for employees and visitors must be published and easy to understand. The guideline for testing must be established by resources and processes available locally now, not later in the year.

STEP 3: Entry Assessment

Entry Assessment is fundamentally necessary. This is the point where all people converge to return to work or enter as a visitor and or customer. The entry is a logical delineation point for administering and managing all the STEPS policy and procedures.

STEP 4: Privacy Policy

Properly managing high risk individuals, as it pertains to the testing and screening policy and procedures, is very challenging. These individuals need to be segregated from the general entry processes in order in insure their health and privacy.

STEP 5: Stay Home and Work-From-Home

Stay Home and Work-from-Home if done correctly can be the lifesaving piece to the STEPS Partnership with America program. This is in effect a safety relief valve for companies and employees where this makes sense.

STEPS
a partnership with
AMERICA

EXPLANATION OF EACH OF THE STEPS

SOCIAL DISTANCING POLICY

Social Distancing Policy has already been implemented across all States. The guidelines can be changed over time and having this be the first step in the Partnership with America creates a starting point that almost all Americans agree upon.

What is social distancing?

Social distancing, also called "physical distancing," means keeping space between yourself and other people outside of your home. To practice social or physical distancing:

- Stay at least 6 feet (2 meters) from other people
- Do not gather in groups
- Stay out of crowded places and avoid mass gatherings

In addition to everyday steps to prevent COVID-19, keeping space between you and others is one of the best tools we have to avoid being exposed to this virus and slowing its spread locally, across the country and world.

When COVID-19 is spreading in your area, everyone should limit close contact with individuals outside your household in indoor and outdoor spaces. Since people can spread the virus before they know they are sick, it is important to stay away from others when possible, even if you have no symptoms. Social distancing is especially important for people who are at higher risk of getting very sick.

Why practice social distancing?

COVID-19 spreads mainly among people who are in close contact (within about 6 feet) for a prolonged period. Spread happens when an infected person coughs, sneezes, or talks, and droplets from their mouth or nose are launched into the air and land in the mouths or noses of people nearby. The droplets can also be inhaled into the lungs. Recent studies indicate that people who are infected but do not have symptoms likely also play a role in the spread of COVID-19.

It may be possible that a person can get COVID-19 by touching a surface or object that has the virus on it and then touching their own mouth, nose, or eyes. However, this is not thought to be the main way the virus spreads. COVID-19 can live for hours or days on a surface, depending on factors such as sun light and humidity. Social distancing helps limit contact with infected people and contaminated surfaces.

Although the risk of severe illness may be different for everyone, anyone can get and spread COVID-19. Everyone has a role to play in slowing the spread and protecting themselves, their family, and their community.

Tips for social distancing

Follow guidance from authorities where you live.

- If you need to shop for food or medicine at the grocery store or pharmacy, stay at least 6 feet away from others.
    - Use mail-order for medications, if possible.
    - Consider a grocery delivery service.
    - Cover your mouth and nose with a cloth face cover when around others, including when you have to go out in public, for example to the grocery store.

- Stay at least 6 feet from others, even when you wear a face covering.

- Avoid large and small gatherings in private places and public spaces, such a friend's house, parks, restaurants, shops, or any other place. This advice applies to people of any age, including teens and younger adults.

- Children should not have in-person playdates while school is out. Help maintain social connections while social distancing through phone and video calls or pen pal letters. Learn tips to keep children healthy while school's out.

- Work from home when possible.

- If possible, avoid using any kind of public transportation, ridesharing, or taxis.

- If you are a student or parent, talk to your school about options for digital/distance learning.

TESTING GUIDELINES

Testing Guidelines for employees and visitors must be published and easy to understand. The guideline for testing must be established to align with resources and processes available locally now, not later in the year. Leverage what can be done effectively by May/June 1, 2020, not the third or fourth quarter of 2020.

- When I return to work, what's going to happen?
- Am I going to be screened, or am I reporting to work just as always?
- If I'm screened, what happens if I test positive or inconclusive?
- What is the screening process and what are my rights?
- Can I opt out of screening and/or can I request additional screening?
- If I'm at work and believe someone else is sick, what can, or should I do?
- What are the restroom policies?
- What are the common areas or food area policies?

- Americans need to know in advance of any return to work - how, where, and when do I receive testing; and how is the test paid for. If it's simple for me, then it means everyone else who may need a test is getting a test just like me.

- It is imperative that the Partnership with American clearly stipulates what will be done immediately, not later. Create a clear two-step process for articulating each one of the STEPS, particularly Testing. Focus on what is simple to do today, now!

- Motivate business leaders to follow basic and common-sense guidelines that can be communicated in advance of returning to work. Alleviate the need for every company having to make it up as they go. Follow the laws tied to drug testing and consistency will prevail across almost all domains.

- Testing guidelines must protect all rights as currently defined by law. Although HIPPA, FDA Regulations, Privacy Identity Laws, ADA, and other industry specific regulations are not simple for all Americans to Understand, we must post a "Testing Bill of Rights" that utilizes the existing privacy laws as universal guidelines.

• All individuals which are determined to have an elevated temperature will be asked if they can give identification and sign a release for their information to pass to the appropriate local medical agencies. In the case of the person who does not give their identification that person can only be documented as a person with a high temperature. In both cases they will be given a phone number tied to their local CDC/HHS agency, asked to leave the premise, and given instructions to shelter in place in Quarantine until they can be tested.

TESTING BILL OF RIGHTS

Employees are entitled to a written policy prior to returning to work or during the on-boarding process. A copy of Testing Bill of Rights is included on page 16 of this document.

STEPS a partnership with AMERICA

Testing Bill of Rights

1. **Written Policy:**
Employees are entitled to a written policy prior to returning to work or during the on-boarding process

2. **Temperature Testing using the STEPS program**
A published list of preconditions is required. All individuals are asked when either submitting as a visitor online or in person in writing or verbally "Are there any conditions that would prevent you from entering the work environment that could be adversely affected by UV light, and potential COVID-19 interaction? Also, while entering the facility, you will be captured in a non-identifiable image which will determine body temperature, and will this be acceptable?"

3. **Conduct pre-employment and re-entering the workforce testing**
Pre-employment testing is considered the most legally valid form of COVID-19 temperature and antibody testing and should be conducted on all applicants as part of the re-entry screening process. However, the test should be requested and administered only after a conditional offer of employment has been made. According to the Americans With Disabilities Act, it is illegal for any employer to test a job applicant without first making a contingent offer.

4. **Test one, test all. Test randomly or with reasonable suspicion**
To avoid claims of discrimination, all applicants who have been extended an offer of employment or re-entry should be subject to testing. If you test only the applicants deemed suspicious, it may be construed as singling out people based on race, gender, or other protected status. Testing of random employees is also acceptable if the selection process is deemed blind.

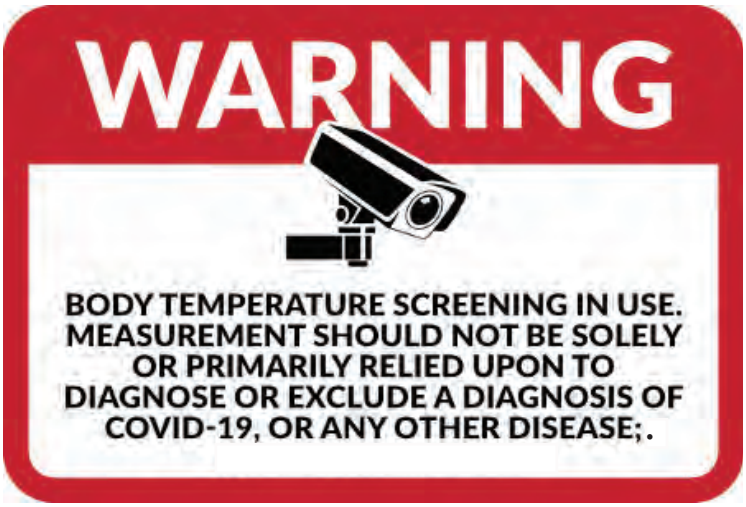
5. **Reasonable-suspicion testing**
Reasonable-suspicion testing is conducted when an employee exhibits potential signs of illness that leads you to suspect the person may have COVID-19. Having a written policy which clearly defines what constitutes suspicious illness helps avoid claims of discrimination. Reasonable suspicion testing after returning to the workplace reduces costs by only testing those employees deemed suspicious.

6. **Maintain confidentiality**
Covid19 test results, like all medical information about your employees, should be kept confidential. To help maintain confidentiality, collect samples in a private and unobtrusive manner and discuss positive test results and consequences with the employee in private.

7. **Work from home agreement paid leave and 48hr paid for testing**
Based on preconditions defined in the CDC guidelines it is important to establish a work from home standard which allows for those who have been tested positive to either receive paid leave or tasks which can be done from home during the two-week quarantine period. Also, if a person is tested with an elevated temperature, the person shall receive two-day paid leave to allow that person to go to a qualified testing facility approved by the CDC or your employer.

8. **Right to choose your family Physician**
If a person is a defined high risk and has reason to suspect COVID-19 contraction, the person shall receive paid leave according to your companies employment policies to allow that person to go to a qualified testing facility approved by the CDC, employer, or family doctor.

9. **Testing costs and procedures**
All testing will be covered by the employer, Insurance provider, state, or local jurisdiction and or agency. The testing must be designed in advance to coordinate with existing company insurance plans and policies.



ENTRY ASSESSMENT PROGRAM (EAP)

Entry Assessment is fundamentally necessary. This is the point where all people converge to return to work or enter as a visitor and/or customer. The entry is a logical delineation point for administering and managing all the STEPS policies and procedures. The nature of the COVID-19 virus dictates this.

This is also an area in which new policy and procedure frontiers are being explored; where all regulations pertaining to NFPA-72, ANSI-156, ADA, HIPPA, Identity Privacy, GDPR, FDA Regulations, and State or local ordinances are going to be challenged and encapsulate the greatest potential liabilities. This is where People, Process, and Technology all come together for either the good of the organization or to its detriment.

How does entry assessment integrate with all the other parts of the STEPS Partnership with America?

Social Distancing Policy

Throughput rates will be dramatically affected and must be understood to manage social distancing. Revolving doors are different than automatic sliding doors or manual swing doors. Elevators pose a real challenge, while certain security entrances (optical turnstiles) are typically “hands-free”. Structured work start times and staggered lunch schedules may be necessary to design flow rates that meet and maximize the Social Distancing effectiveness.

Testing and Screening

Entry points are the optimal converged areas to educate workers and visitors, and implement screening and testing guidelines. This is a real convergence of People, Process, and Technology. This will, in some cases, be pushed to outside the facility and will include environmental, technology implementation, and privacy challenges.

Privacy Policy (PP)

Properly managing high risk individuals, as it pertains to the testing and screening policy and procedures, is very challenging. These individuals who qualify for special treatment need to be segregated from the general entry processes in order in insure their health and privacy. Individuals who suffer from crones, or ongoing cancer treatment, challenging pregnancies, or HIV all need confidentiality and protections above and beyond the general workforce population. This is an area of Partnership that requires individual company administration and personal responsibility from the employee.

Stay Home and Work-from-Home (WFH)

Work-from-Home if done correctly can be the lifesaving piece of the STEPS Partnership with America program. This is in effect a safety relief valve for companies and employees where it makes sense. From a disease management prospective, this initiative is highly feasible and effective. However, the challenges for managers to effectively supervise remote people is real. WFH can incrementally assist with managing at-risk individuals and throughput, and social distancing guidelines.

The Entry Assessment is a specifically designed section of the bSMART® assessment methodology and software tool developed by Butchko, Inc.

The bSMART® entry assessment module has been adapted to the STEPS program for mass deployment, utilizes pre-built data models to account for business and industry, public or private, architectural design, entry design types, and use cases. The bSMART® entry assessment module is a subset of the full bSMART® Vulnerability and Risk Assessment system utilized to provide a dynamic real-time business resiliency, risk management, and maturing of operations posture.

STEPS a partnership with AMERICA

b-SMART® ENTRY THROUGHPUT TRACKER ESI convergent

ENTRANCE NAME:	Building One, Main Entrance
ENTRANCE DESCRIPTION:	Manual revolving door(s), Manual single swing doors, no vestibule
ENTRANCE CONDITIONS:	Social Distancing
ENTRANCE TYPE:	Public Entrance

	INBOUND PPM		OUTBOUND PPM	
Morning (AM) ↑	10		2	↓ Morning (AM)
Mid-day (2-way) ↓↑	1		1	↓↑ Mid-day (2-way)
Evening (PM) ↑	2		10	↓ Evening (PM)
Peak Time	12		12	Peak Time
Average	4.3		4.3	Average
MAX	12		12	MAX
Efficiency Rating	36.1%		36.1%	

The bSMART® Entry Assessment provides a consistent and repeatable process that rapidly characterizes existing conditions and delivers practical recommendations for safe operations improvement. User proficiency is with minimal training due to the engineered process upon which it is designed.

PRIVACY POLICY (PP)

Properly managing high risk individuals, as it pertains to the testing and screening policy and procedures, is very challenging. These individuals need to be segregated from the general entry processes in order in insure their health and privacy.

Individuals who suffer from crones, or ongoing cancer treatment, challenging pregnancies, or HIV all need confidentiality and protections above and beyond the general workforce population. These potentially lethal circumstances require employees taking personal responsibility and HR administrators to work within the laws, but vigilantly extending special privileges when deemed necessary and afforded under the law.

U.S. Department of Health & Human Services must be the guiding force for the testing and establishment of national guidelines for COVID-19 testing in the workplace. This document also establishes a Bill of Rights that center around current processes to protect individuals surrounding Drug Testing standards and State laws. This process best applies to COVID-19 with respect to governance and policies and procedures that protect the rights of an individual.

It is evident that unless there is a zero tolerance for infection spread in the workplace, as is the use of drugs based on the safety of others, there will be a reluctance for the workforce to reenter the workplace. We believe this is the most effective roadmap to help agencies as well as states define the rights attributed to the protection of individuals. These are the seven points used to develop the above "Testing Bill of Rights", and assistance simplifying the Privacy Policy Program for protecting employers and individual your rights.

1. Draft a written policy

2. Temperature testing using the STEPS program

A list of preconditions that would be part of the list that is published, including: All individuals are asked when either submitting, as a visitor online or in person, in writing or verbally "Are there any conditions that would prevent you from entering the work environment that could be adversely affected by UV light and potential COVID-19 interaction? Also, while entering you will be captured in a non-identifiable image which will determine body temperature and will this be acceptable upon entry?"

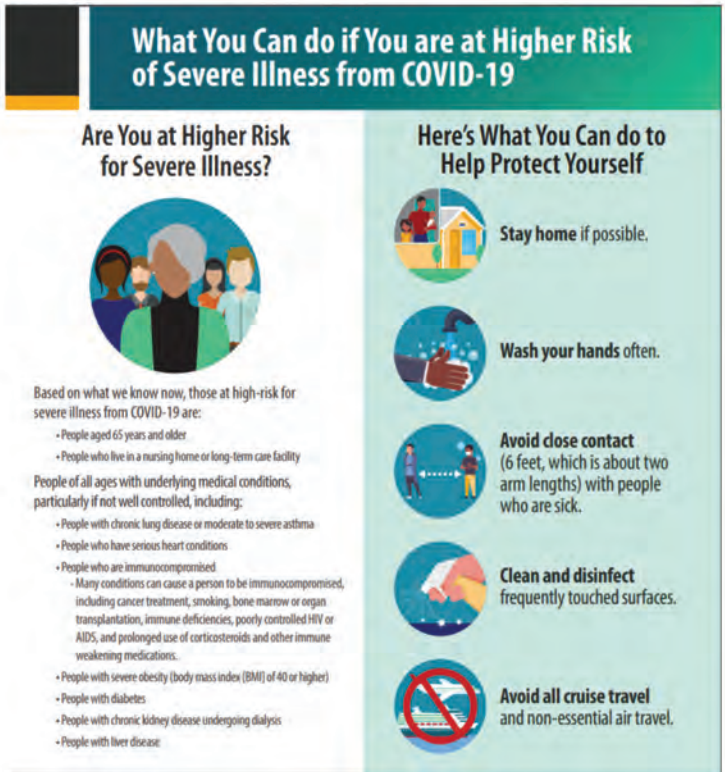
Visitor
All individuals which are determined to have an elevated temperature will be asked if they can give identification and sign a release for their information to pass to the appropriate local medical agencies. In the case of the person who does not give their identification that person can only be documented as a person with a high temperature. In both cases they will be given a phone number tied to their local CDC/HHS agency, asked to leave the premise, and given instructions to shelter in place in Quarantine until they can be tested.

Employee
All individuals that are employee or tenants will work with their HR facilitator who is working with union representatives as well as managers to ensure that all documents have been either agreed upon with respect to the STEPS program and the elevated temperature testing protocol. Those who do not accept the entry process will be given the opportunity to work from home at 100% compensation without prejudice. Those who agree will be allowed to return using this process. No employee will have to specifically define the reasons for their unwillingness to return. Under the Privacy Bill of Rights each individual has right to freely decide whether they agree to the process of re-entering the workspace.

The HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

Provide a statement reference to the use of testing in respect to HIPAA /HITRUST privacy concerns. It is the intent of the testing and the bSMART® assessment to define the proper process of entry into a work environment based on circumstances and configuration of an entity's workplace and or structure. The ability to define an individual's current health status is only based on a preliminary evaluation using either skin surface temperature or other method and will not initially tie to an individual's identity without consent. Consent may occur if asked and the individual has the right to decline, however the individual, based on current and future CDC and HHS orders, may be asked to leave the premise and be given recommendations to visit a local clinic, hospital or be given a phone number to call so that they receive the proper protocol to shelter in place based on prevailing Quarantine practices.



STAY HOME AND WORK-FROM-HOME (WFH)

Stay Home and Work-from-Home, if done correctly, can be the lifesaving piece to the STEPS Partnership with America program. This is in effect a safety relief valve for companies and employees where this makes sense. From a disease management prospective, this initiative is highly feasible and effective. However, the challenges for managers to effectively supervise remote people is real. WFH can incrementally assist with managing high-risk individuals, throughput reductions for entry, testing and screening, and social distancing guidelines.

WFH STEPS Solutions

There are solutions that you can deploy today. IT teams are absolutely experts on what solutions are practical, appropriate and effective. Encourage them and help them be successful at supporting managers now faced with the ominous task of remote work space management.

- You must ensure that a secured communication infrastructure is immediately deployed.
    - Assign company laptops to defined groups.
    - MiFi communications when large data files are not required.
    - Consider private cellular networks (new and effective with the emerging 5G networks)

- Employees must have multifactor authentication turned on, with hopefully some form of challenge question attached to a separate device such as a phone. By having all remote employees doing this, you are creating a work at home culture and discipline that allows supervisors to better manage and challenge compliance.

- The employer must immediately create a security awareness program that has employees go thru a tutorial of work-from-home rules DAILY. Such as; DO NOT CLICK ON ANY ATTACHMENTS UNLESS YOU CHALLENGE THE SENDER! Again, this creates a way for supervisors to monitor work at home discipline improvement.

- Increase the protection levels of firewalls and sniffers on all your systems to make it as inconvenient as possible for your work at home employee to receive emails that are flagged by the business entity.

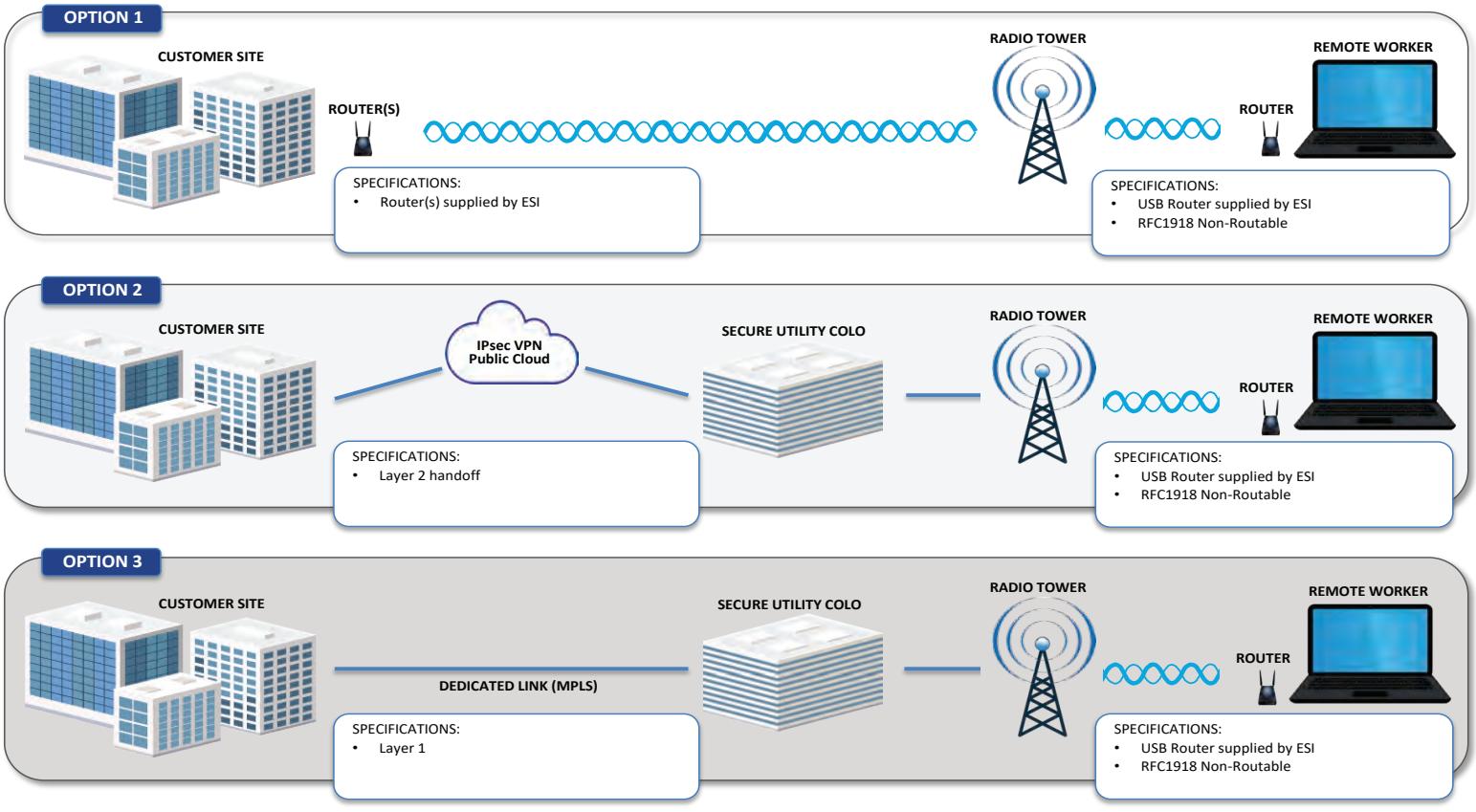
- Reevaluate permissions structures within remote employee groupings. Segment whenever possible.

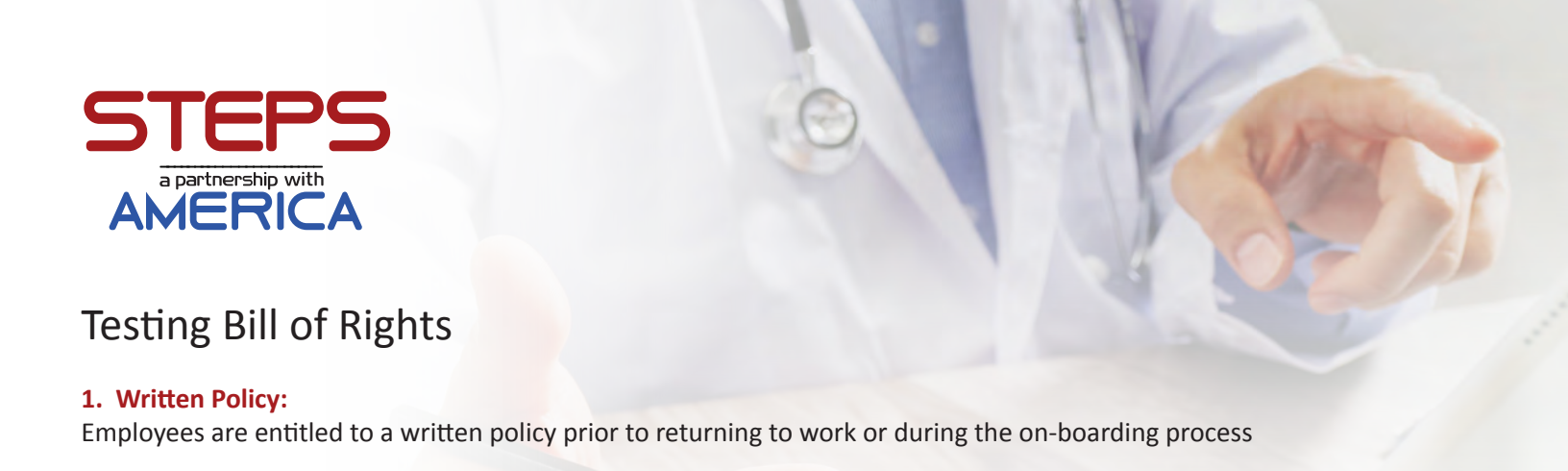
These basic rules dramatically improve liability posture and may just save the network and business from Ransomware attacks. This is the converged application of People, Process, and Technology to maximize usability in a safe and secure manner. If the business wasn't already operating in a converged manner, COVID-19 just made sure that it is.

The Work-from-Home basis for concern:

Organizations are facing great challenges as more than 70% of workforces are now working in unfamiliar and unsupervised environments. In fact, it is their home in which they may not have ever worked before. This becomes a great issue with regards to the efficiency and effectiveness of those who have never been in a position where they have not been directly supervised. This has become one of the most daunting tasks for an executive management team as well as those who support the team, both procedurally and technologically. Most organizations have built management systems and technology infrastructure to support operations within the four walls of their facilities they work in and not extensively outside those walls.

Most organizations had an average of 15% of their organization that was specialized in their roles and responsibilities that traveled and/or worked remotely. The systems that were created for this remote work force had been tested and true. Even with that measure of infrastructure there were vulnerabilities. The human factor was always the one element that was very challenging and difficult to control. With this dramatic shift in workforce to home the scale of imminent problems has risen. There are three main issues that will potentially create the greatest risks to businesses in the post COVID-19 world, and that is the technological gap at home, policy and procedure adherence, and finally human nature and the human inconsistency, all of which could be adequately controlled previously within the four walls.





Testing Bill of Rights

1. Written Policy:
Employees are entitled to a written policy prior to returning to work or during the on-boarding process

2. Temperature Testing using the STEPS program
A published list of preconditions is required. All individuals are asked when either submitting as a visitor online or in person in writing or verbally "Are there any conditions that would prevent you from entering the work environment that could be adversely affected by UV light, and potential COVID-19 interaction? Also, while entering the facility, you will be captured in a non-identifiable image which will determine body temperature, and will this be acceptable?"

3. Conduct pre-employment and re-entering the workforce testing
Pre-employment testing is considered the most legally valid form of COVID-19 temperature and antibody testing and should be conducted on all applicants as part of the re-entry screening process. However, the test should be requested and administered only after a conditional offer of employment has been made. According to the Americans With Disabilities Act, it is illegal for any employer to test a job applicant without first making a contingent offer.

4. Test one, test all. Test randomly or with reasonable suspicion
To avoid claims of discrimination, all applicants who have been extended an offer of employment or re-entry should be subject to testing. If you test only the applicants deemed suspicious, it may be construed as singling out people based on race, gender, or other protected status. Testing of random employees is also acceptable if the selection process is deemed blind.

5. Reasonable-suspicion testing
Reasonable-suspicion testing is conducted when an employee exhibits potential signs of illness that leads you to suspect the person may have COVID-19. Having a written policy which clearly defines what constitutes suspicious illness helps avoid claims of discrimination. Reasonable suspicion testing after returning to the workplace reduces costs by only testing those employees deemed suspicious.

6. Maintain confidentiality
Covid19 test results, like all medical information about your employees, should be kept confidential. To help maintain confidentiality, collect samples in a private and unobtrusive manner and discuss positive test results and consequences with the employee in private.

7. Work from home agreement paid leave and 48hr paid for testing
Based on preconditions defined in the CDC guidelines it is important to establish a work from home standard which allows for those who have been tested positive to either receive paid leave or tasks which can be done from home during the two-week quarantine period. Also, if a person is tested with an elevated temperature, the person shall receive two-day paid leave to allow that person to go to a qualified testing facility approved by the CDC or your employer.

8. Right to choose your family Physician
If a person is a defined high risk and has reason to suspect COVID-19 contraction, the person shall receive paid leave according to your companies employment policies to allow that person to go to a qualified testing facility approved by the CDC, employer, or family doctor.

9. Testing costs and procedures
All testing will be covered by the employer, Insurance provider, state, or local jurisdiction and or agency. The testing must be designed in advance to coordinate with existing company insurance plans and policies.

STEPS
a partnership with
AMERICA

RESEARCH AND DETAILS BEHIND THE STEPS

Partnering with Americans to get America Back to Work:

Social Distancing Policy (CDC defined and implemented)
Testing Guidelines for employees and visitors (Drug testing legal precedent)
Entry Assessment Program (EAP) bSMART®
Privacy Policy (PP) properly managing high risk individuals
Stay Home and Work-From-Home Incentive Program (WFH)

Federal/State Guidelines
Gov't Medical Alliances
Consulting Groups
Existing Regulation Applied
Gov't/Private Partnership

Creating a partnership with Americans is all about taking the right S.T.E.P.S. Partnering with Americans to get America Back to Work is not a slogan, but a process of building confidence and trust. STEPS is a "Partnership with America" to do everything that is necessary and feasible right now to ensure that the right STEPS are being taken to protect health, privacy, and wellbeing. The greatest challenge is doing the right things now, and not allowing missteps and future mistakes to erode momentum in getting Americans back to work. With all the miss-information, negative information, and social media influences, it is necessary to put forth a plan that substantially alleviates or eliminates any reasons not to go back to work. In this way, people who are skeptical and fearful of returning to work can be reassured that the right STEPS are being taken to assure their health, privacy and wellbeing. The partnership must be common sensical and easy to understand. The STEPS taken must be done consistently and visibly. Any facility that puts forth publicly the "STEPS" moniker, is letting Americans know that the five easy to understand steps that are applicable to their business or facility are in practice.

STEP ONE: Social Distancing

Social Distancing Policy has already been implemented across all States. The guidelines can be changed over time and having this be the first step in the Partnership with America creates a starting point that almost all Americans agree upon.

STEP TWO: Testing Guidelines

Testing Guidelines for employees and visitors must be published and easy to understand. The guideline for testing must be established by resources and processes available locally now, not later in the year. What can be done effectively by May/June 1, 2020, not the third or fourth quarter of 2020.

- When I return to work, what's going to happen?
- Am I going to be screened, or am I reporting to work just as always?
- If I'm screened, what happens if I test positive?
- What is the screening process and what are my rights?
- Can I opt out of screening and or can I request additional screening?
- If I'm at work and believe someone else is sick, what can, or should I do?
- What are the restroom policies?
- What are the common areas or food area policies?

a. Americans need to know in advance of any return to work - how, where, and when do I receive testing; and how is the test paid for. If it's simple for me, then it means everyone else who may need a test is getting a test just like me.
b. It is imperative that the Partnership with American clearly stipulates what will be done now, not later. Create a clear two-step process for articulating each one of the STEPS, particularly Testing. Focus on what is simple to do today, now!
c. Motivate business leaders to follow basic and common-sense guidelines that can be communicated in advance of returning to work. Alleviate the need for every company having to make it up as they go. Follow the laws tied to drug testing and consistency will prevail across almost all domains.
d. Testing guidelines must protect all rights as currently defined by law. Although HIPPA, FDA Regulations, Privacy Identity Laws, ADA, and other industry specific regulations are not simple for all Americans to Understand, we must post a "Testing Bill of Rights" that utilizes the existing privacy laws as universal guidelines.

Testing Bill of Rights

1. **Written Policy:**
   Employees are entitled to a written policy prior to returning to work or during the on-boarding process

2. **Temperature Testing using the STEPS program**
   A published list of preconditions is required. All individuals are asked when either submitting as a visitor online or in person in writing or verbally "Are there any conditions that would prevent you from entering the work environment that could be adversely affected by UV light, and potential COVID-19 interaction? Also, while entering the facility, you will be captured in a non-identifiable image which will determine body temperature, and will this be acceptable?"

3. **Conduct pre-employment and re-entering the workforce testing**
   Pre-employment testing is considered the most legally valid form of COVID-19 temperature and antibody testing and should be conducted on all applicants as part of the re-entering screening process. However, the test should be requested and administered only after a conditional offer of employment has been made. According to the Americans With Disabilities Act, it is illegal for any employer to test a job applicant without first making a contingent offer.

4. **Test one, test all. Test randomly or with reasonable suspicion**
   To avoid claims of discrimination, all applicants who have been extended an offer of employment or re-entry should be subject to testing. If you test only the applicants deemed suspicious, it may be construed as singling out people based on race, gender, or other protected status. Testing of random employees is also acceptable if the selection process is deemedmblind.

5. **Reasonable-suspicion testing**
   Reasonable-suspicion testing is conducted when an employee exhibits potential signs of illness that leads you to suspect the person may have COVID-19. Having a written policy which clearly defines what constitutes suspicious illness helps avoid claims of discrimination. Reasonable suspicion testing after returning to the workplace reduces costs by only testing those employees deemed suspicious.

6. **Maintain confidentiality**
   COVID-19 test results, like all medical information about your employees, should be kept confidential. To help maintain confidentiality, collect samples in a private and unobtrusive manner and discuss positive test results and consequences with the employee in private.

7. **Work from home agreement paid leave and 48hr paid for testing**
   Based on preconditions defined in the CDC guidelines it is important to establish a work from home standard which allows for those who have been tested positive to either receive paid leave or tasks which can be done from home during the two week quarantine period. Also, if a person is tested with an elevated temperature, the person shall receive two-day paid leave to allow that person to go to a qualified testing facility approved by the CDC or employer.

8. **Right to choose your family Physician**
   If a person is a defined high risk and has reason to suspect COVID-19 contraction, the person shall receive paid leave according to your companies employment policies to allow that person to go to a qualified testing facility approved by the CDC, employer, or family doctor.

9. **Testing costs and procedures**
   All testing will be covered by the employer, Insurance provider, state, or local jurisdiction and/or agency. The testing must be designed in advance to coordinate with existing company insurance plans and policies.

e. All individuals which are determined to have an elevated temperature will be asked if they can give identification and sign a release for their information to pass to the appropriate local medical agencies. In both cases they will be given a phone number tied to their local CDC/HHS agency and be given instructions to shelter in place in Quarantine until they can be tested. In the case of the person who does not give their identification that person can only be documented as a person with a high temperature and will be asked to leave the premise as well as the person giving consent.

STEP THREE: Entry Assessments

Entry Assessment is fundamentally necessary. This is the point where all people converge to return to work or enter as a visitor and or customer. The entry is a logical delineation point for administering and managing all the STEPS policy and procedures. The nature of COVID-19 virus dictates this. This is also an area in which new policy and procedure frontiers are being explored; where all regulations pertaining to NFPA-72, ANSI-156, ADA, HIPPA, Identity Privacy GDPR, FDA Regulations and State or local ordinances are going to be challenged and encapsulate the greatest potential liabilities. This is where People, Process, and Technology all come together for either the good of the organization or for its detriment.

How does entry assessment integrate with all the other parts of the STEPS Partnership with America?

Social Distancing: Throughput rates will be dramatically affected and must be understood to manage social distancing. Revolving doors are different than automatic sliding doors or manual swing doors. Elevators pose a real challenge, while certain security entrances (optical turnstiles) are typically “hands-free”. Structured work start times and staggered lunch schedules may be necessary to design flow rates that meet and maximize the Social Distancing guidelines.

Testing and Screening: Entry points are the optimal converged areas to educate workers and visitors and implement screening and testing guidelines. This is a real convergence of People, Process, and Technology. This will potentially in some cases be pushed to outside the facility and will include environmental, technology implementation, and privacy challenges.

Privacy Policy (PP): Properly managing high risk individuals, as it pertains to the testing and screening policy and procedures, is very challenging. These individuals who qualify for special treatment need to be segregated from the general entry processes in order in insure their health and privacy. Individuals who suffer from crones, or ongoing cancer treatment, challenging pregnancies, or HID all need confidentiality and protections above and beyond the general workforce population. This is an area of Partnership that requires individual company administration and personal responsibility from the employee.

Stay Home and Work-from-Home (WFH): Work-from-Home if done correctly can be the lifesaving piece to the STEPS Partnership with America program. This is in effect a safety relief valve for companies and employees where this makes sense. From a disease management prospective, this initiative is highly feasible and effective. However, the challenges for managers to effectively supervise remote people is real. WFH can incrementally assist with managing PPP individuals and throughput social distancing guidelines.

The Entry Assessment is a specifically designed section of the bSMART® assessment methodology and software tool developed by Butchko, Inc. The bSMART® entry assessment module has been adapted to the STEPS program for mass deployment, utilizes pre-built data models to account for business and industry, public or private, architectural design, entry design types, and use cases.

The bSMART® entry assessment module is a subset of the full bSMART® Vulnerability and Risk Assessment system utilized to provide a dynamic real-time business resiliency, risk management, and maturing of operations posture. The bSMART® Entry Assessment provides a consistent and repeatable process that rapidly characterizes existing conditions and delivers practical recommendations for safe operations improvement. User proficiency is with minimal training due to the engineering process upon which it is designed.

Below is an outline of how the bSMART® process is structured.

bSMART® Entry Assessment Module: Pre-assessment

- Pre-assessment evaluation
    - Characterize entry areas – online bSMART® survey to response which streamlines data collection to tailor indus try-specific models to site-specific locations
        - Physical barriers (outer and inner perimeter)
        - Surrounding layout – available space inside and outside of the perimeter barrier
        - Airflow characteristics and isolation options
        - Entry type and operation
        - Personnel throughput; Existing access controls and processes
        - User profile (i.e. public access or restricted, children, adults, materials delivery, special needs, etc.)
        - Area layout and configuration (enclosed, indoor vs outdoor, HVAC characteristics, etc.)
    - Civil / Environmental conditions
        - Parking Pedestrian Flow Routes
        - Public Transportation Flow Routes
        - ADA Entrance Accessibility Evaluation, Exterior
        - Building Exterior Entry Routes
    - Medical facilities proximities Complimentary Information requests
        - Photos of building perimeter and entries
        - Site/Building layout drawings – start with architectural drawing
    - Pre-analyze each situation regarding existing risk and guideline protection situation. Define areas in need of additional evaluation, develop preliminary list of protection enhancement recommendations.
- Final Assessment
    - Address Pre-Analysis results through additional information gathering and on-site assessment.
    - Produce refined enhancement recommendations that are practical and realistic

Architectural Building and Facilities Categories

- Public Access
    - Temporary Venues – Outdoor festivals, amateur sporting events (runs, triathlons, bike races)
    - Large Event – Sports Stadiums, Mega churches
    - Small Event – Movie Theaters, Concert Halls, Churches
    - Large Shopping – Shopping Malls, Grocery Stores, Large Retail
    - Small Shopping – Convenience Stores, Single Storefronts.
    - Campus – mixed public and private access
- Private / Restricted
    - Single Tenant
        - Manufacturing
        - Distribution
        - Corporate Office
        - Campus
        - Public transport – airport TSA, subway & train stations, bus terminals
    - Multi-Tenant
        - Corporate Office
        - Manufacturing
        - Campus
- Medical (See above building types) Special assessment charges by facility
- Pharmacies. Template for remote assessment. No Charge
- Restaurants. Template for remote assessment. No Charge
- Small Shopping – Convenience Stores, Single Storefronts. Template for remote assessment. No Charge

Pre-Assessment Facility Review:

- Hours of Operation
    - 12 hours, daytime hours
    - 24 hours, 7 days per week
    - Two shift or Three shift facilities
    - Other

- Special Access Areas, Power Plants and Maintenance
    - General public access, back door policies
    - Badged, no registration
    - Badged, registration required
    - Technology review
    - Other

- Supply Logistics and Vehicle Management
    - Manned
    - Unmanned
    - Verification
    - Unverified
    - Controlled parking
    - Free space parking
    - Technology review
    - U.S Postal, FedEx, UPS and similar services process and procedures

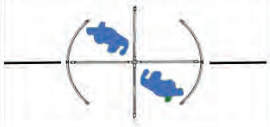
Facility Entrance Designs
- Model each of these designs in advance.
    - Public
    - Private
    - Public and Private
- Description, purpose/use, security options/provisions, regulatory issues
- Drawings and illustrations
- Common recommendations and options for social distancing
- Procedure templates

Pre-assessment/Site-assessment

b-SMART® ENTRY THROUGHPUT TRACKER

ESI convergent

ENTRANCE NAME:	Building One, Main Entrance
ENTRANCE DESCRIPTION:	Manual revolving door(s), Manual single swing doors, no vestibule
ENTRANCE CONDITIONS:	Social Distancing
ENTRANCE TYPE:	Public Entrance

	INBOUND PPM ↑		↓ OUTBOUND PPM	
Morning (AM) ↑	10		2	↓ Morning (AM)
Mid-day (2-way) ↓↑	1		1	↓↑ Mid-day (2-way)
Evening (PM) ↑	2		10	↓ Evening (PM)
Peak Time	12		12	Peak Time
Average	4.3		4.3	Average
MAX	12		12	MAX
Efficiency Rating	36.1%		36.1%	

THROUGHPUT TRACKER ENTRY ALLOWANCES AND CALCULATIONS

STEPS a partnership with AMERICA

Building Perimeter Door Types	PPM Allowance One Direction	PPM Allowance Two Directions	# Units	Total PPM AM/PM	Total PPM Lunch	Social Distance PPM Allowance One Direction	Social Distance PPM Allowance Two Directions	# Units	Total PPM AM/PM	Total PPM Lunch
Manual Swing Door 1-way	20		0	0		10		0	0	
Manual Swing Door 2-way		15	0		0		5	0		0
Manual Swing Door vestibule 1-way	10		0	0		5		0	0	
Manual Swing Door vestibule 2-way		5	0		0		3	0		0
Manual Swing Door w/ ADA Operator 1-way	15		0			10		0	0	
Manual Swing Door w/ ADA Operator 2-way		10	0	0	0		5	0		0
Manual Swing Door vestibule w/ ADA Operator 1-way	5		0			3		0	0	
Manual Swing Door vestibule w/ ADA Operator 2-way		2	0	0	0		3	0		0
Auto Swing Door 1-way	20		0			10		0	0	
Auto Swing Door 2-way		15	0		0		8	0		0
Auto Swing Door vestibule 1-way	10		0	0		5		0	0	
Auto Swing Door vestibule 2-way		5	0		0		3	0		0
Auto Sliding Door 1-way	20		0	0		10		0	0	
Auto Sliding Door 2-way		40	0	0	0		10	0	0	0
Auto Sliding Door vestibule 1-way	15		0	0		10		0	0	
Auto Sliding Door vestibule 2-way		30	0	0	0		10	0	0	0
Manual Revolving Door	18	18	0	0	0	8	8	0	0	0
Small Auto Revolving Door (up to 12'0")	18	18	0	0	0	8	8	0	0	0
Large Auto Revolving Door (Over 12'0")	27	27	0	0	0	10	10	0	0	0
Security Revolving Door	16	16	0	0	0	8	8	0	0	0
TOTAL				0	0				0	0

Lobby Access Control Types	PPM Allowance One Direction	PPM Allowance Two Directions	# Units	Total PPM AM/PM	Total PPM Lunch	Social Distance PPM Allowance One Direction	Social Distance PPM Allowance Two Directions	# Units	Total PPM AM/PM	Total PPM Lunch
Manual Turnstile 1-way	12					6				
Manual Turnstile 2-way	8					4				
Optical Turnstile 1-way	12					6				
Optical Turnstile 2-way	8					4				
Auto Swing Gate 1-way	6					3				
Auto Swing Gate 2-way	3					3				
Security Revolving Door	16					8				
Security Portal (Mantrap)	4					4				
TOTAL				0	0				0	0

Visitor Management Systems

The Visitor Management Process into our Entry Assessment process is to validate the HR, IT and Security requirements necessary to build confidence and trust in STEPS. According to the industry leading visitor management system provider, Building Intelligence, there are different rights and privileges that belong to employees Vs. guests or visitors which are outlined in the visitor management process.

- Known Employee
- Known Supplier (regular long-term badged contract worker)
- Known Guest (specific short-term purpose intermittent visit)
- Unknown

According to Building Intelligence, each of the four groups of visitors to any public, private or hybrid public/private facility will have existing policy and procedures that must be augmented for the STEPS program.

Known Employees have an existing policy and procedure that is tied to HR and are conditional terms of employment. These employees are subject to an on-boarding process that includes IT, Operational Technology (OT) and Physical Security (PS) permissions that are tied to identity management policies. The HR, IT, and PS managers will inherently decide how STEPS is applied legally.

Known Suppliers are bound by the rule and regulations of their own employers, which may have changed as a result of STEPS; and must adhere to the policies and procedures of the facility they are performing work. This is where a STEPS adherence program really makes it easier to protect rights and privileges and eliminates much of the confusion surrounding the entry access programs. These suppliers or contract workers are subjected to the same on-boarding and day-to-day process as employees.

Known Guests are granted access for one day or less for a specific meeting or reason. On-line, kiosk, or visitor desk registration all require Known Guests to read, acknowledge and agree to new STEPS health guidelines, and company policies and procedures. Traditionally these guests have been escorted by a Known Employee or a Known Supplier which is even more critical now.

Unknown is very common in a public building and by its very nature may never know the identity or specific reason for the visit. However, in a private or hybrid public/private facility it is critical to have a way to manage unknown visitors that protect all aspects of the enterprise. A publicized nationally implemented STEPS program would significantly reduce the training and adherence costs associated with interfacing with these individuals as well as the three other groups. They are determined to have or not have a valid reason for being in the facility and are processed in as a known visitor or are asked or required to exit and follow the proper procedures in the future. Considering the damage, a willingly or unwillingly sick individual can do if obtaining unauthorized access within a facility, this may now fall under the bio terrorist guidelines set forth by Title 22 of the US Code, Section 2656f(d) This makes the guidelines and strategy for managing entry even more important. Businesses who have in the past deployed detection strategies only, now need to decide how to protect their security teams and employees. Business that utilize prevention strategies are in a stronger compliance posture and make it easier to compartmentalize dealing with unknown visitors. Undoubtedly, this will change the open campus culture of many organizations in the future.

HVAC Entry Assessment Impact

The traditional entry assessment models focus on security tied to business resiliency and do not need to consider air flow management. In the case of bio terrorism or pandemic environments the paradigm significantly changes. So, as part of our bSMART® entry assessment we have made available a team of subject matter experts. The mission statement for the air flow assessment group and for this part of the analysis is SME review only. This group does not do site visits as part of the original entry assessment.

This group reviews:

- Mechanical Ductwork Drawings
- Temperature Controls Drawings
- Specified "Sequence of Operations" for HVAC Equipment
- HVAC Equipment Schedules
- HVAC Equipment Submittals
- Air Balance Reports
- Previous third-party reports that were created as part of the original design documents
- Post installation inspections

This SME group can listen in on meetings with the existing building Maintenance Staff, Temperature Controls Contractors, System Integrators, or HVAC providers and direct questions when applicable; listen to and review recommendations from existing service providers and render opinions regarding the quality of claims, proposed decisions and action plans.

Entry assessments that result in entrances being utilized more "hands-free" that now open automatically and hold open longer need to evaluate how this may change air flow dynamics in areas that may have screening and testing. In an ideal world we would create a negative air pressure compartment in the screening and testing areas to evacuate the air out of the compartment as designed to minimize head and face exposure and create a positive pressure zone surrounding the negative zone to prevent air exfiltration and proliferation into the other areas. This type of complex (and expensive) system is commonly reserved for infectious isolation in hospitals, clean rooms and biomedical laboratories. In the real world, acting quickly, we can only look at making adjustments that maximize what the existing building system can do, and not focus on what it can't. Our group of SMEs' all have decades of real-world application and field experience and can provide guidance in discussions regarding what are potentially the best placement of specific screening processes. They can also guide discussions about realistic general workspace management guidelines.

Things to consider:

- Existing ductwork design establishing HVAC zoning. (Critical in establishing separate air flow zones to prevent cross zone mixing).
- Existing Systems performance accomplished design goals. (Is the existing HAVC and Controls System operating as specified by the design; can be precisely determined by Retro commissioning, or RCx).
- Existing equipment capabilities including; Airflow Capacity, Outside Air Percent Capacity, Heating and Cooling Sections Capacities. (How much available additional capacity - if any - exists with the installed equipment).
- Existing Equipment variable operational capabilities. (Does existing equipment have the capability to provide variable capacity output).
- Temperature Controls Design; Sensor Capabilities and Placements, HVAC Equipment Control Points, limits of control. (Does the existing temperature controls system installed have capability for changing the sequence of operations if required).
- Energy and Operational Costs (How will changing the way Equipment operates effect utility invoices and maintenance operations).

Medical Equipment and Procedures as part of Entry Assessment:

This will be the most challenging piece to fill with SME's from the ESI Team perspective. It is possible that we can perhaps bring people to our group from the FDA, or perhaps an insurance Board of Advisors member can bring a SME to our group who's persona is respected. My fear is we will end up with only manufacturer SME's based off solutions that assessment clients are considering. The role of this SME is to evaluate the medical implications of people evaluation, testing, and entry screening procedures. This may be a role that we need to look for a third-party group that already exists for the purposes of this initiative. Below is a link to FEMA that allows companies to look at sourcing or building a supply chain around approved equipment.
https://www.fema.gov/fema-supply-chain-task-force-leads-four

STEP FOUR: Privacy Policy (PP)

Privacy Policy (PP): Properly managing high risk individuals, as it pertains to the testing and screening policy and procedures, is very challenging. These individuals need to be segregated from the general entry processes in order in insure their health and privacy. Individuals who suffer from crones, or ongoing cancer treatment, challenging pregnancies, or HID all need confidentiality and protections above and beyond the general workforce population. These potentially lethal circumstances require employees taking personal responsibility and HR administrators to work within the laws, but vigilantly extending special privileges when deemed necessary and afforded under the law .

U.S. Department of Health & Human Services must be the guiding force for the testing and establishment of national guidelines for COVID-19 testing in the workplace. This document also establishes a Bill of Rights that center around current processes to protect individuals surrounding Drug Testing standards and State laws. This process best applies to COVID-19 with respect to governance and policies and procedures that protect the rights of an individual. It is evident that unless there is a zero tolerance for infection spread in the workplace as is the use of drugs based on the safety of others there will be a reluctance for the workforce to reenter the workplace. We believe this is the most affective roadmap to help agencies as well as states to define the rights attributed to the protection of individuals. This is the seven points used to develop the above “Testing Bill of Rights”, and assistance simplifying the Privacy Policy Program for protecting employers and individual your rights.

1. Draft a written policy
Adopting COVID-19 language to existing written policies assures employers that they are communicating guidelines consistent with existing guidelines for “Drug Testing” within your existing jurisdictions. Having a written policy in place is the single most important step in setting up your company’s COVID-19 testing procedures. Work with your legal counsel to develop and implement a policy in accordance with applicable state laws. This will allow you to notify potential hires early in the application process and obtain their consent before testing.

2. Temperature Testing using the STEPS program
In the process of using the STEPS Partnership with America program there must be a clearly defined use of the system with an individual’s rights. Protecting rights of the individual and their preconditions must be defined. STEPS goal is to provide the rights afforded to you the employer and employees by HIPAA, California Privacy Act, and GDPR. The following document will define how this will take place and following the proper process we will lay the foundation to establish controls necessary to insure the persons privacy rights are protected.

A list of preconditions that would be part of the list that is published would be. All individuals are asked when either submitting as a visitor online or in person in writing or verbally “Are there any conditions that would prevent you from entering the work environment that could be adversely affected by UV light, and potential COVID-19 interaction? Also, while entering you will be captured in a non-identifiable image which will determine body temperature and will this be acceptable upon entry?”

Visitor: All individuals which are determined to have a temperature will be asked if they can give identification and sign a release for their information to pass to the appropriate local medical agencies. In both cases they will be given a phone number tied to their local CDC/HHS agency and be given instructions to shelter in place in Quarantine until they can be tested. In the case of the person who does not give their identification that person can only be documented as a person with a high temperature and will be asked to leave the premise as well as the person giving consent. The individual which gave consent may get a call from their local CDC/HHS agency to get information regarding testing locations or be sent a self-test packet.

Employee: All individuals that are employee or tenants will work with their HR facilitator who is working with union representatives as well as managers to ensure that all documents have been either agreed upon with respect to the STEPS program and the temperature testing protocol. Those who do not accept the entry process will be given the opportunity to work from home at 100% without prejudice. Those who agree will be allowed to return using this process. No employee will have to specifically define the reasons for their unwillingness to return. Under the Privacy Bill of Rights each individual has right to freely decide whether they agree to the process of re-entering the workspace.

The HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

Statement reference to the use of temperature testing in respect to HIPAA /HITRUST privacy concerns. It is the intent of the temperature testing and bSMART® Assessment to define the proper process of entry into a work environment based on circumstance's and configuration of an entity's workplace and or structure. The ability to define an individual's current health status is only based on a preliminary evaluation using either skin surface temperature or other and will not initially tie to an individual's identity without consent. Consent may occur if asked and the individual has the right to decline however the individual based on current and future CDC and HHS orders may be asked to leave the premise and be given recommendations to visit a local clinic, hospital or be given a phone number to call so that they receive the proper protocol to shelter in place based on prevailing Quarantine practices.

1. Conduct pre-employment and re-entering the workforce testing
Pre-employment testing is considered the most legally valid form of COVID-19 temperature and antibody testing and should be conducted on all applicants as part of the screening process. However, the test should be requested and administered only after a conditional offer of employment has been made. According to the Americans With Disabilities Act, it is illegal for any employer to test a job applicant without first making a contingent offer.

2. Test one, test all
All employee must test to re-enter the workforce to determine the best process for managing those with the antibody and those without. This may be a way to separate or segment the workforce population. As stated under testing process this is to control spread and to give those with pre-existing conditions as well as the most vulnerable the ability to activate the work from home process. To avoid claims of discrimination, all applicants who have been extended an offer of employment should be subject to testing. If you test only the applicants deemed suspicious, it may be construed as singling out people based on race, gender, or other protected status.

3. Understand your COVID-19 testing options
In general, there are two types of legally accepted drug testing methods.

- Random temperature testing is conducted unannounced on all current employees or a class of employees (e.g., employees who drive for company business) and provides the best deterrent against spread because nobody knows when he or she will be tested. The upside of random testing is that individuals can feel reassured that the person next to you is potentially free of illness.
- Reasonable-suspicion testing is conducted when an employee exhibits potential signs of illness that leads you to suspect the person may have COVID-19. Having a written policy which clearly defines what constitutes suspicious illness help avoid claims of discrimination. Reasonable suspicion testing also helps you avoid creating a "Big Brother" atmosphere in the workplace and reduces costs by only testing those employees deemed suspicious.

Comply with your state law(s)
As previously mentioned, many states have enacted restrictions on COVID-19 testing in the workplace. We have provided a great link below from Sciteck.org that breaks down the laws, state-by-state

This document uses each state's drug testing laws as the foundation for national testing laws for COVID-19.

4. Maintain confidentiality
COVID-19 test results, like all medical information about your employees, should be kept confidential. To help maintain confidentiality, collect samples in a private and unobtrusive manner and discuss positive test results and consequences with the employee in private.

5. Work from home agreement (LCA) paid leave and 48hr paid for testing
Based on preconditions defined in the CDC guidelines it is important to establish a work from home standard which allows for those who have been tested positive to either receive paid leave or tasks which can be done from home during the two-week quarantine period. Also if a person is tested with a temperature the person shall receive two day paid leave to allow that person to go to a qualified testing facility approved by the CDC such as LabCorp https://www.labcorp.com/coronavirus-disease-covid-19.

https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/people-at-higher-risk.html
https://www.cdc.gov/coronavirus/2019-ncov/downloads/COVID19-What-You-Can-Do-High-Risk.pdf

Testing costs and procedures
All testing will be covered by the employer, Insurance provider, state, or local jurisdiction and or agency. The testing must be designed in advance to coordinate with temperature processes. As stated in the STEPS program.

Application of Drug-free Workplace to COVID-19 free work place Federal Laws and Regulations Numerous federal requirements govern COVID-19-free workplace policies. There is no requirement for most private employers to have a drug-free workplace policy of any kind. The exceptions to this are federal contractors and grantees, as well as safety- and security-sensitive industries and positions.

Federal statutes on drug-free workplace policies can be divided into two broad groups, or categories, of legislation. One category includes laws such as the Drug-free Workplace Act of 1988. These laws are designed explicitly to target workplace substance use. They legally compel certain types of employers to take action against drug use in the workplace, such as by developing a written policy.

The other category includes laws designed to protect the basic civil rights of American workers. These statutes provide special legal protections to certain kinds of employees. They set clear limits on how far an employer can go in investigating and establishing consequences for employee drug use. The most important federal laws and regulations of this type to consider are:

- The Americans with Disabilities Act (ADA) of 1990
- The Civil Rights Act of 1964
- The Family and Medical Leave Act (FMLA) of 1993
- The National Labor Relations Act (NRLA) of 1935

For employers considering drug testing, legal counsel is advisable, because lawsuits have been filed against employers for invasion of privacy, wrongful discharge, defamation, and discrimination. The best way to avoid getting drawn into litigation, aside from securing legal counsel, is to make sure that all of your policies are implemented fairly and consistently—in a manner that does not conflict with any federal, state, or local civil rights or workers' rights laws. For more information on legal best practices, review 10 Steps for Avoiding Legal Problems.

Americans With Disabilities Act (ADA) of 1990

The Americans With Disabilities Act (ADA) is perhaps the most important federal civil rights legislation that affects employers when developing and implementing drug-free workplace policies. It prohibits all U.S. employers with more than 15 employees from discriminating against qualified job applicants and employees because of a physical disability.

The ADA does not, in any way, prohibit employers from having a drug-free workplace policy, nor does it provide any special protection to individuals who are currently using illegal drugs. However, it does make it illegal for employers to discriminate against recovering alcoholics and drug users who have already sought treatment for their addiction.
Under the terms of the ADA:

- Employers cannot fire, refuse to hire, or refuse to promote someone simply because she/he has history of substance use.
- Employers also cannot fire, refuse to hire, or refuse to promote employees merely because they are enrolled in a drug or alcohol rehabilitation program.

Employers who have drug-testing programs need to be extremely careful not to single out employees for testing simply because they look or act as though they are under the influence of drugs or alcohol. Many of the physical symptoms that are commonly associated with intoxication—slurred speech, disorientation, or a lack of coordination—can also be the result of a serious physical disability or medical condition, such as diabetes, low blood sugar, or mental illness. Individuals with these conditions are protected under the provisions of the ADA. Singling them out for testing or disciplinary action could result in charges of discrimination. Finally, employers should refrain from asking employees about their legal prescription drug use as part of the pre-hiring or pre-promotion drug-testing process. While the case law in this area is still evolving, some state courts have ruled that requesting such information constitutes a form of discrimination and is in violation of the ADA.

Alleged violations of the ADA account for almost half of all lawsuits involving drug-free workplace programs, so it is extremely important for employers to acquaint themselves with the details of this legislation. Additional information about the ADA can be obtained by contacting the Department of Justice's (DOJ) ADA hotline at 800-514-0301 or accessing DOJ's ADA Information and Technical Assistance website.

Civil Rights Act of 1964

The Civil Rights Act, 28 Code of Federal Regulations (CFR), 42 is a landmark law that prohibits private employers with 15 or more employees from discriminating against individuals on the basis of race, sex, religion, or nationality. Employers implement a drug-free workplace policy need to keep in mind Title VII of the Civil Rights Act. While challenges to drug testing or drug-free workplace policies under this legislation are relatively rare, employers should make sure that their programs treat all workers equally and avoid singling out any particular racial, ethnic, or gender group for testing or disciplinary action.

In large workplaces that are racially and ethnically diverse, it is also wise to involve a diverse and representative group of employees in formulating your policy. This will help ensure that you produce a program that is culturally competent, fairly enforced, and sensitive to the needs of all employees.
More information on Title VII of the Civil Rights Act is available from the Equal Employment Opportunity Commission (EEOC).

Family and Medical Leave Act (FMLA) of 1993

The Family and Medical Leave Act (FMLA) (PL 103-3) applies to all public agencies and to private employers with more than 50 workers. Under FMLA, these employers must allow employees who have worked for the employer for at least one year and who have worked at least 1,250 hours in the past 12 months to take up to 12 weeks of unpaid, job-protected leave because of their own serious health condition or to care for a spouse, child, or parent who has a serious health condition. Eligible employees may use their FMLA leave to deal with substance use disorders and related problems, including:

- Treatment of drug or alcohol addiction
- Treatment of another physical illness or incapacity related to substance use (such as kidney failure)
- Caring for a close family member who is undergoing treatment for these conditions

FMLA also prohibits employers from retaliating against workers who request FMLA leave. For example, an employer cannot demote, fire, or refuse promotion to an employee simply because that employee takes 12 weeks off for treatment of a substance use disorder. Employers also are prohibited from taking any action against workers who request time off to care for addicted family members. For more information, visit the Department of Labor's (DOL) FMLA guide.

The National Labor Relations Act (NRLA) of 1935

Employers implementing drug-free workplace policies in unionized workplaces need to be aware of the requirements of the National Labor Relations Act (NRLA). Passed in 1935, this law provides a legal framework for all management and labor negotiations. Under NRLA, any drug-testing program affecting unionized workers must be negotiated and agreed on with the union through a formal collective bargaining process. Even when an employer is required to implement a drug-testing program by another federal mandate, such as the Omnibus Transportation Employee Testing Act of 1991, the employer must negotiate with the union to determine exactly when testing will be conducted and what penalties should apply to workers who test positive for drug or alcohol use. All too often, employers assume that negotiating a drug-testing agreement or drug-free workplace policy with their unions will be an unpleasant and adversarial process. However, some unions actually support such programs because of their potential to reduce workplace injuries and accidents.

More information on how employers can work collaboratively with unions is available from the National Labor Relations Board (NLRB).

STEP FIVE: Stay Home and Work-from-Home (WFH)

Stay Home and Work-from-Home (WFH): Work-from-Home if done correctly can be the lifesaving piece to the STEPS Partnership with America program. This is in effect a safety relief valve for companies and employees where this makes sense. From a disease management prospective, this initiative is highly feasible and effective. However, the challenges for managers to effectively supervise remote people is real. WFH can incrementally assist with managing PPP individuals, throughput reductions for entry, testing and screening, and social distancing guidelines.

WFH STEPS Solutions:
There are solutions that you can deploy today. The IT teams are absolutely experts on what to do within the four walls. Encourage them and help them be successful at supporting the managers now faced with the ominous task of remote work space management.

1. You must ensure that a secured communication infrastructure is immediately deployed.
    a. Assign company laptops to defined groups.
    b. MiFi communications when large data files are not required.
    c. Consider private cellular networks (new and effective with the coming of 5G)

2. Employees must have MFA multi authenticated permissions turned on with hopefully some form of challenge question attached to a separate device such as a phone. By having all remote employees doing this, you are creating a work at home culture and discipline that allows supervisors to better manage and challenge compliance.

3. The employer must immediately create a security awareness program that has employees go thru a tutorial of work-from-home rules DAILY. Such as; DO NOT CLICK ON ANY ATTACHMENTS UNLESS YOU CHALLENGE THE SENDER! Again, this creates a way for supervisors to monitor work at home discipline improvement.

4. I would toggle up the firewalls and sniffers on all your systems to make it inconvenient as possible for your work at home employee to receive emails that are flagged by the business entity.

5. Reevaluate your permissions structures within your remote employee groupings. Segment whenever possible.
These basic rules will dramatically improve your liability posture and may just save your network and your business from Ransomware attacks. This is the age-old triumvirate of People, Process, and Technology which are the key elements in converged thought and operations is the real answer for today. If you were not already, you are now part of that converged world. COVID-19 just made sure of that.

The reasons for real concern operationally and organizationally

Organizations are facing great challenges as more than 70% of workforces are now working in unfamiliar and unsupervised environments. In fact, it is their home where they may not have ever worked before. This becomes a great issue with regards to the efficiency and effectiveness of those who have never been in a position where they have not been directly supervised. This has become one of the most daunting tasks for an executive management team as well as those who support the team, both procedurally and technologically. As we may know most organizations have built management systems and technology infrastructure to support operations within the four walls of their facilities they work in and not extensively outside those walls. Most organizations had an average of 15% of their organization that was specialized in their roles and responsibilities that traveled and or worked remotely. The systems that were created for this remote work force had been tested and true. Even with that measure of infrastructure there were vulnerabilities that occurred. The human factor was always the one equation that was very challenging and difficult to control. With this dramatic shift in workforce to home we now have many imminent problems that will arise. There are three main issues that will potentially create the greatest risks to businesses in the post COVID-19 world and that is the technological gap from home, policy and procedure adherence, and finally human nature and the human inconsistency, all of which could be adequately controlled previously within the four walls.

Technological WFH Gap

Technology that has been developed to communicate on a LAN network typically has been either designed or evolved infrastructure with firewalls, cyber tools, and rules sets built to define and recognize and resolve vulnerabilities, otherwise referred to as a "kill-chain". These vulnerabilities could easily be detected and quarantined or enclaved. Most organizations established a process of internal communication as well as segmentation at least for those who have evolved to a more mature IT posture. The problem today is you have a work force that no longer is protected by the infrastructures we created internally to protect the business from the internal users. When at an instance, many employees who do not have all their familiar "work space" technology, especially the communication technology necessary to securely connect to the internal network, this becomes a recipe for disaster. Reflexively, the inexpensive and quick solution is using a router attached to a Spectrum or Cox communication Wi-Fi, which was previously thought to be good enough. Unfortunately, what may happen is "Business" intellectual property will be streamed over an unsecured Wi-Fi with a password "MYDOGGYISPRETTY1234" especially when their dogs name is Pretty and your children have posted this on every social networking chat room for the past 3 years. Out of necessity, companies are having their employee's sign into the VPN from home; however, they are using the family Wi-Fi router which is still a recipe for disaster. The problem is we have no choice since you didn't have a dedicated laptop to send them home with that had all the secured encryption to protect the data at rest. The reality is that on their personal laptop, it is unfortunate that they have either accidently or intentionally watched hours of very questionable content; or have let their kids play every downloadable free game from the internet that have viruses and backdoors to every nation state syndicate and hacker in the deep web.

https://nypost.com/https://www.cbsnews.com/news/zoom-bombing-calls-hacked-racial-slurs-pornography/2020/03/31/fbi-warns-of-hackers-hijacking-online-zoom-meetings-classes/

Policy and Procedure Adherence

Policies and procedures that have been built by companies as part of disaster recovery plans, compliance requirements, continuity of operation plans, risk mitigation strategies and business continuity plans were rarely built for work from home. Again, as I have mentioned most of this was built to support a business within four walls. The major issue is that most organizations do not have policies established to run a business from afar nor do they have procedures that allow for proper guidance by managers or executives from a distance. As we move into months two, three, and four of this difficult and horrible event in world history, the managers will begin the process of finding effective ways to manage; and without the policies and procedures to do so there will be an imminent struggle with following his or her guidance. With regards to regulated markets such as energy, banking, or manufacturing, you must follow policies and procedures set forth by customers and governing bodies. Although there is an immediate relaxing and lack of concern for regulations since everyone is in triage mode, you as an organization will inevitably be held responsible for any breaches that occur due to your lack of adherence. As highlighted by the link provided in the technology gap above, face-to-face time is a necessary and important part of adherence. However, important aspects of the adherence were dictated by work space oversight by supervisors. Inevitably, if the technology gap cannot be solved; how can managers implement work space policy and procedures remotely that will meet your compliance?

Human Inconsistency

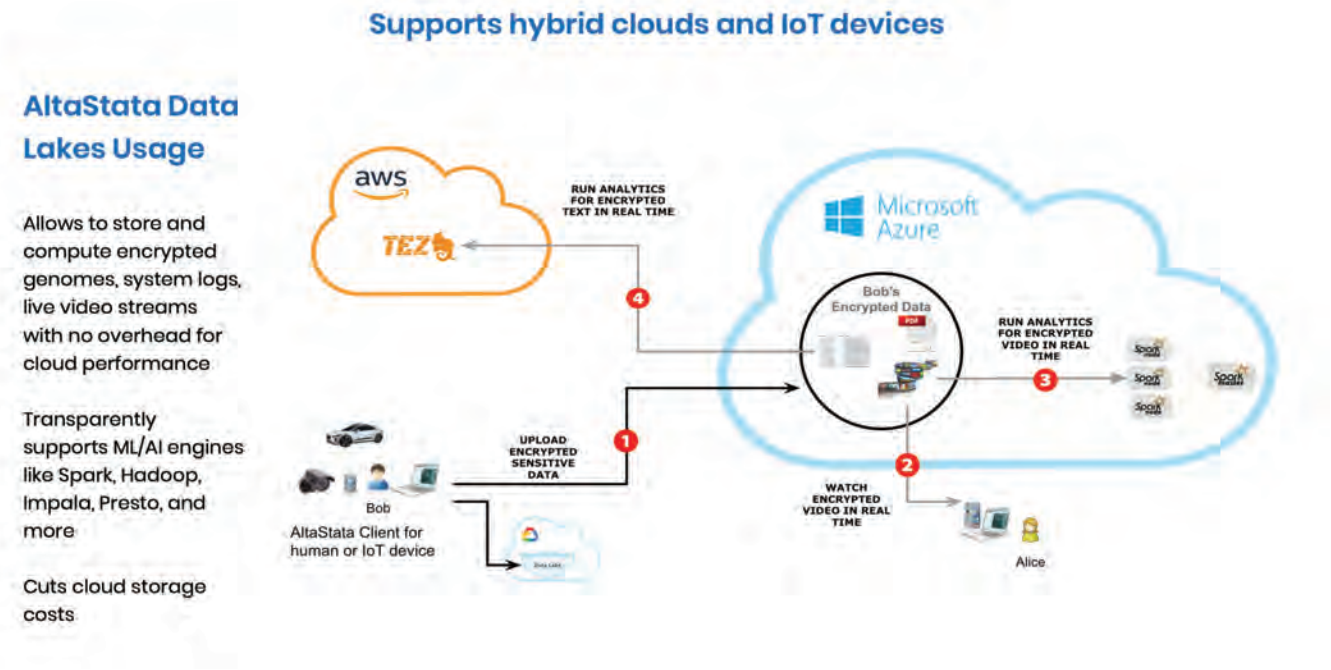
For as long as we have had employees required to attend work, they have been waking up in the morning, maybe they took a shower, and then got dressed (appropriately) and arrived ready to work. Well that's not happening anytime soon. So, with that in mind now employees wake up, do not take a shower, and do not get dressed appropriately other than maybe a respectable t-shirt and then turns on his or her computer. Are these employees really ready to work? This is the first issue related to being unsupervised and this is just the first step. The issue is the work from home discipline. It takes years to establish not only how to work from home but what to work on from home to become productive. It's not just your employees that need to be disciplined, but the dog and others who live in the home. Unfortunately, the work at home human factor also is the greatest weakness in productivity and proficiency. The issue is connectivity and the answer now is Web ex, Microsoft Team, Go to Meeting, Zoom, Skype and others.

Unfortunately, this too becomes a minefield since most employees do not have the proficiency to operate in this environment securely. Most of the time they begin loading the site with as many slide decks, excel sheets, and manufacturing diagrams as they can so they can bring them up to share with their other employees from home. That's admirable, however how does a supervisor manage the work space rules remotely, especially as it pertains to company intellectual property? Unfortunately, the human tendency at home is to be lazy and would prefer to take as many shortcuts as possible to get the job done. To be honest, the 15% of your workforce that always works remotely, does not always dress properly; does not always follow policy and procedures; and over time does become more tech-savvy and secure. But the numbers are lower, so the risk is lower. Now the math says you're in trouble.

The following includes two excellent solutions for implementing WFH Cyber Hygiene and Secure Communications policies.

1. Work-from-Home (WFH) Program: AltaStata applied to existing mature VPN access configs

AltaStata MIT startup provides an independent way to protect sensitive and personal data in the cloud from internal and external breaches using the client-side encryption. The approach does not require reprogramming of the existing Big Data solutions and tools does not reduce performance or scalability of the cloud and can be implemented in days. In addition, personal data protection as part of a general cloud strategy can define the one to one relationship to data while ensuring that data in transit and at rest are secured to the individual user while establishing proper key permission at the administrative level.



If you look closely at the above diagram, AltaStata can prevent the most dangerous type of attacks by malicious insiders and or more commonly user's mistakes; which is a problem not addressed by other cloud vendors due to their typical shared security responsibility model. In the case of AltaStata each file is encrypted using its own data key, which in the end may help to protect organizations from appearing in the news due to massive data breaches. The elimination of the traditional administrator shared security responsibility model simplifies the process and perfects the secure channel communications and data-at-rest issues facing the other cloud vendors. It's difficult to assess at this early stage, but I think we also can agree that the new normal work-from-home models makes this method of encrypting each file with its own data key mistake proof.

Cost Structure RMR pricing model
AltaStata uses a flexible pricing model that is tailored to your data usage and number of access users.

AltaStata allows work from home users to perform encryption on their edge devices, so that transmitted and stored images, documents, and videos remain secure within the organization's cloud storage, from both external and internal threats. Using AltaStata, organizations let their employees WFH while securely storing and sharing the documents within the organization's public cloud account. Additionally, organizations can enable their customers to securely manage their personal sensitive data within the organization's public cloud account and it does not require VPN access. Here's a comparison:

Encryption - Traditional Cloud Data Lakes Based on cloud server-side encryption, which protects data at rest from external hackers and cloud vendor access	Encryption - AltaStata Data Lakes Based on client-side encryption to protect the organization against both outsider and insider threats. Through AltaStata users manage their personal data within protected personal boxes in the cloud object storage and authorize other users and programs to access their encrypted files or live video streams
Performance - Traditional Cloud Data Lakes This approach allows fast processing of stored data using the ML/AI ecosystem tools	Performance - AltaStata Data Lakes This approach supports fast upload, streaming, random access and parallel encrypted data processing using ML/AI ecosystem tools like Spark with no overhead for cloud scalability and performance. The approach also reduces cloud storage costs through data compression
Data Security - Traditional Cloud Data Lakes Organization's admins and some users have excessive privileges to access and modify sensitive data, which constitutes an insider threat	Data Security - AltaStata Data Lakes Organization's sysadmin and CISO do not constitute an insider threat, however they can control and restrict data access for end users and perform formal data audit. This method complies with the GDPR and CCPA approach for personal data privacy

2. Work-from-Home (WFH) Program: SecurePCN applied to existing overburdened VPN remote access configs

SecurePCN is not a MiFi and not a secure mobile phone hotspot, which operates fairly securely within the open public cellular channel. SecurePCN delivers a true secure private cellular network with a priority LTE connection, segregated on the back-end of all U.S. mobile carrier networks – not the open public channel, and more importantly, not the Internet. Remote connection to the Secure Private Network is fortified by a bank-grade firewall, updated in real time to defend against upstream and downstream threats.

Simplified Connection
Sign up for the service, plug a Secure Utility IBB Router into your home computer or work issued laptop and it automatically connects to the strongest network to operate over the back-net cellular infrastructure anywhere in North America. Secure PCN establishes a connection for interconnected terminals which allows work from home employee to securely login and connect across a private cellular network. This eliminates the need for layers of secured communication (VPN). Employees can remotely connect from anywhere in North America with a Palo Alto firewall at the edge. The patented IBB router can also be pinged regularly to ensure stability with security.

BENEFITS

- Continuity of Operations with no added infrastructure or management costs
- Immediately deployable with little to no training.
- No additional monitoring tools or oversight training
- The elimination of Cisco Any Connect or Palo Alto Global Project per user costs
- No additional security layers needed to be segmented and secure
- No conflicting end points and no work needed at end points
- Home Internet is eliminated, along with all the home end point security and band width issues
- The elimination of almost all Tier One tech support needs
- Future enabled with no legacy issues

FDA "Does Not Intend to Object" To Unapproved Fever Detection Cameras
By: Charles Rollet, Published on Apr 17, 2020

The US FDA has declared it will not go after the many companies marketing unapproved fever detection cameras during the coronavirus public health emergency, even though it does consider these products medical devices, it has announced in new guidance.

The guidance comes after weeks of uncertainty about the legal status of these products, which traditionally require FDA 510(k) clearance prior to being marketed/sold. But that has not stopped numerous firms from touting unapproved cameras as they cash in on a pandemic-induced Gold Rush.

However, in order to "help address urgent public health concerns", the FDA is now saying it "does not intend to object" to the distribution of unapproved fever detection cameras, although this leniency will "remain in effect only for the duration of the [COVID-19] public health emergency".

In this note, IPVM examines this new announcement and its impacts closely, including:

- Background: FDA Regulation of Fever Screening Cameras
- FDA New Thermal Camera Enforcement Policy Announced
- FDA Reasoning: Fighting Shortage
- Policy Only Temporary
- Fever Cams Still Medical Devices
- Winner Dahua, Loser Hikvision
- Other Winners And Losers
- New Entrants
- Risk of Shoddy Products Spreading

Background: FDA Regulation of Fever Screening Cameras
As IPVM reported last month, the FDA considers body temp screening cams (paired with a thermometer to confirm the fever) to be medical devices, technically a "Telethermographic system intended for adjunctive diagnostic screening". These require FDA 510(k) clearance before being marketed, a process that takes around 130 days.

FDA Announces It Won't Enforce Its Own Regulations
However, the FDA announced new guidance yesterday (April 16) stating it will temporarily "not intend to object" to those selling such cameras without 510(k) clearance:
To help ensure the availability of products that might offer benefit to health care providers and the general public during the public health emergency, FDA does not intend to object to the distribution and use of telethermographic systems intended for initial body temperature assessment for triage use [emphasis added]

The FDA has released a 10-page enforcement policy labeled 'contains nonbinding recommendations':

Enforcement Policy for Telethermographic Systems During the Coronavirus Disease 2019 (COVID-19) Public Health Emergency Guidance for Industry and Food and Drug Administration Staff April 2020

FDA Reasoning: Fighting Shortage

The FDA said it is doing this as it wants to address the shortage of such devices:
FDA believes the policy set forth in this guidance may help address urgent public health concerns raised by shortages of temperature measurement products by helping to clarify the regulatory landscape and expand the availability of telethermographic systems used for initial body temperature measurements for triage use during this public health emergency. [emphasis added]

Policy Only Temporary

The FDA emphasized that this guidance is temporary:
This policy is intended to remain in effect only for the duration of the public health emergency related to COVID-19 declared by HHS
There is no indication of when HHS will declare COVID-19 to no longer be a public health emergency; yesterday, an-all time high of over 2,400 Americans died from the virus and over 500,000 have tested positive so far.
The last US public health emergency was Swine Flu, which lasted well over a year - it was declared in April 2009 and ended in June 2010. Given COVID-19's greater impact, it will likely last at least as long, if not significantly longer.

Fever Cams Considered Medical Devices

Despite some companies falsely claiming their fever cameras are somehow not medical devices, in this guidance, the FDA clearly states that it does consider these products medical devices and under its regulatory purview:
Telethermographic systems are devices when they are intended for a medical purpose, such as measurement of the self-emanating infrared radiation that reveals the relative temperature variations of the surface of the body
Generally, telethermographic systems fall within the definition of a device when they are intended for a medical purpose
This means that companies selling these systems will still need 510(k) clearance to sell fever detection cameras once the pandemic is over. However, the money for them is likely to be made in the immediate future.

FDA Recommendation: Only Use With Thermometer

While the FDA said that 510(k) clearance is temporarily waived, it did state this was as long as the cameras are for "triage use", i.e. the cameras are paired with a body thermometer to confirm whether the person actually has a fever:
An elevated body temperature measurement is confirmed in the context of use with secondary evaluation methods (e.g., non-contact infrared thermometer (NCIT) or clinical grade contact thermometer)

FDA Testing/Labeling Recommendations

The FDA also recommended the fever cams are "tested and labeled consistent with the following ISO standard: IEC 80601-2-59:2017" or any "alternative performance specifications that provide similar results to IEC 80601-2-59:2017".
The FDA recommended thermal cams are tested under following "performance specifications" including "measurement uncertainty, is less than or equal to ±0.5°C (±0.9°F) over the temperature range of at least 34-39°C (93.2-102.2°F)".

FDA Recommends Cameras Only Used One Person at A Time

The FDA recommended:
should be used to measure only one subject's temperature at a time
The recommendation about only measuring one person's temp at a time goes against some firms, like Sunell's Panda Cam, which tout simultaneous fever detection:

For example, ADI yesterday sent an email saying that WatchNet (Sunell relabeller) can (impossibly) detect 16 people in 1/33 of a second:

> WatchNET's Body Temperature Detection System can detect 16 people's temperature within 30 milliseconds

Prominent Notice Labelling

The FDA says that a 'prominent notice' should be included, explaining:

> The labeling includes a prominent notice that the measurement should not be solely or primarily relied upon to diagnose or exclude a diagnosis of COVID-19, or any other disease;

IPVM has mocked up such a notice:

Long List of Label Recommendations

Moreover, the FDA gave many other label recommendations that should be on the devices in order for users to "better understand the device":

1) The labeling includes a prominent notice that the measurement should not be solely or primarily relied upon to diagnose or exclude a diagnosis of COVID-19, or any other disease;
2) The labeling includes a clear statement that:
   a) Elevated body temperature in the context of use should be confirmed with secondary evaluation methods (e.g., an NCIT or clinical grade contact thermometer);[12]

[10] This is usually a blackbody (idealized physical body that absorbs all incident electromagnetic radiation) with known temperature and emissivity that can be used for thermal drift compensation.
[11] For more information on this recommendation, see Clause 201.14 of IEC 80601-2-59: 2017.
[12] This labeling recommendation is consistent with IEC 80601-2-59: 2017.

Contains Nonbinding Recommendations

   b) Public health officials, through their experience with the device in the particular environment of use, should determine the significance of any fever or elevated temperature based on the skin telethermographic temperature measurement;
   c) The technology should be used to measure only one subject's temperature at a time; and
   d) Visible thermal patterns are only intended for locating the points from which to extract the thermal measurement.
3) The labeling includes a clear description of:
   a) Device performance specifications and the methodology and frequency of any calibration needed to maintain the labeled specifications;[12]
   b) How to use the thermal image to make a temperature measurement to within the stated device accuracy;
   c) A description and purpose of the blackbody reference source (used for thermal drift compensation) and its importance in obtaining an accurate temperature assessment;
   d) The reference body site used for temperature estimation, including any calibration or correction needed to estimate the temperature at that location, and the accuracy of the measurement at the reference site (e.g., oral, tympanic membrane);
   e) How different environmental and system setup factors can affect the measurement, including the body site chosen for measurement, the condition of the screening site (e.g., screening background, ambient temperature and humidity, airflow);[13]
   f) Different factors to consider in the design of the facility protocol (e.g., installation, viewing angle, blackbody temperature reference source);[14]
   g) The installation procedures and qualification testing that should be performed during installation or when imaging equipment is being relocated;[15] and
   h) The appropriate imaging distance based on the spatial resolution and performance of the camera.[16]
4) The labeling references and is consistent with the guidelines in ISO/TR 13154: 2017: *Medical electrical equipment — Deployment, implementation and operational guidelines for identifying febrile humans using a screening thermograph*; and
5) The labeling highlights the differences in design, indications, or functions, as applicable, compared to the unmodified, FDA-cleared version of the product or includes a clear identification that the device is not FDA-cleared or approved.

How or where this long list of labeling should be applied is not made clear. We asked the FDA for feedback and will update with their response.

Recommendations Nonbinding

Despite this long list of recommendations, the FDA states it its advice is not enforceable or required:

In general, FDA's guidance documents, including this guidance, do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word should in Agency guidance means that something is suggested or recommended, but not required.

Risk: Dubious Companies Rewarded

There has been an explosion in firms touting unregulated coronavirus-detection camera solutions. IPVM has counted 49 companies now offering such solutions, of which only a few have 510(k) clearance. Problems included:

- Athena Security faked its coronavirus marketing and is using the wrong kind of camera
- Feevr is also using the wrong kind of camera and when IPVM reported this, they threatened legal action and made false allegations against us
- Dahua also faked its coronavirus marketing

The fact that the FDA has (temporarily) given carte blanche to these unregulated products is a big boost for such firms. But it presents a risk to the public, since often these companies are totally new entrants to the thermal field and do not offer the right kind of camera, setup advice, etc. This could lead to many false positives/negatives and poor implementation.

Analysis: Dahua Winner, Hikvision Winner But Less So

Neither Dahua nor Hikvision had FDA clearance for their thermal products going into this crisis. But Dahua decided to aggressively push fever detection anyway, even faking its marketing, while Hikvision took the more cautious path and avoided doing so in the US (it touts these products internationally, though).

But thanks to this new FDA guidance, Dahua's riskier bet is now looking like a huge winner. The thermal camera market has exploded thanks to the pandemic, with end users frantically seeking to protect clients in any way they can, and Dahua now has a big edge.

Approved Lose Somewhat

FLIR, Optotherm, and all the other established manufacturers who make FDA-cleared fever screening cameras have lost a significant selling point for their products: that they are the only government-approved game in town. On the other hand, those companies have significant backlogs in orders so they are still selling out of everything they can make and clearly getting a big boost from this.

Downside: Encouraging Bad Practices

On the downside, the FDA's new guidance will result in even more dubious thermal solutions being touted, and allow the fever cam Gold Rush to accelerate. Poorly-implemented solutions will likely cause false negatives/positives, leading to unnecessary harassment for regular people. Meanwhile, many will rush to buy the cheapest solution or the one with slickest marketing or simply what they can actually find available.

Another major issue is what will happen when the pandemic is over and the FDA once again requires 510(k) clearance for such solutions. Though, many of these systems may be abandoned by that time anytime.

Upside: Clarity Finally Here, More Companies Can Enter

On the plus side, the FDA's new guidance does offer clarity to a previously fraught situation. Many companies were declining to enter the market due to legal risks. Now, they can join which might help expand options.

UV Technology and Systems

The STEPS team are not medical experts, however we concur that UV will play a major role in mitigating COVID-19. We have copied the following information directly from the RD website.

Why Choosing the Right Ultraviolet Disinfection System Can Save Lives and Money. RD™ UVC system can confirm that the actual lethal UVC dose needed to kill the most serious superbugs and pathogens including Coronavirus and C. diff are delivered to targeted areas. This provides the proof of compliance that you demand that other machines cannot. Hospitals, nursing homes, schools, businesses of all kinds can keep their patients, customers and employees safe with UVC disinfection.

On average, 1.7 million HAIs are reported each year; of these, an estimated 1.2 million were avoidable, according to the CDC. Fortunately, there is an infection prevention tool available that prevents the spread of HAI – Ultraviolet (UVC) disinfection.

UVC disinfection uses UV light to penetrate pathogen cell walls and render them unable to replicate. The best UVC solutions deliver measurable doses that show the exact length of time and intensity required to kill specific microorganisms that cause infections. Once a room is properly treated with UVC light, dangerous pathogens can't reproduce or spread.

https://www.larsonelectronics.com/search/result?w=N95%20IND-HL%20IND-CD%20XLE-MD-BK-CV19-R1%20N95%20Disinfection%20Sanitation%20UVC%2050c%20TBL%20AT%20TM&utm_campaign=7221072644&utm_source=google&utm_medium=cpc&utm_content=430326288155&keyword=%2Buv%20%2Bdisinfection&adgroupid=80646819776&gclid=CjwKCAjw1cX0BRBmEiwAy9tKHonuOXleymnQFhO1mXaFPSRfN7vv9tA-NdG8OCDxVwNib1pdpoN1_RoCit4QAvD_BwE

https://rduvc.com/uv-combat-infection/?gclid=CjwKCAjw1cX0BRBmEiwAy9tKHjRmh1nE0MOlg1bbS2Szv6JqwA61oMjjGh-anUjaYCfDeHEr2q__LBoCW2IQAvD_BwE

https://kapsule.store/

https://www.uvccleaningsystems.com/

COronavirus Measurement and Positive Alert System (COMPAS) for Disease Infection Monitoring and Pandemic Spread

STEPS a partnership with AMERICA

A crucial component to monitoring any infectious disease crisis is the ability to know and track such parameters as infection rates and the geolocation of outbreaks, not only to provide situational awareness of a pandemic, but also to help inform decisions regarding asset and resource allocation.

The Coronavirus Measurement and Positive Alert System (COMPAS) is a COTS-based system designed to safely provide rapid field results and a common operating picture during both natural and manmade emergencies, including disease pandemics (Figure 1). COMPAS is capable of operating as a stand-alone field test solution which can be enhanced by an incident-wide data assimilation, analysis, and situational awareness system. The COMPAS solution is scalable from a single field location to thousands, user friendly, and has reasonably low upfront capital and ongoing operating costs.

The COMPAS field sensor system provides immediate analysis and results indication to operators and consists of a thermal imager, calibration reference, field test controller, and an optional auxiliary data workstation. The touch-free operation and remote set-back deployment flexibility simultaneously maintains safety for test subjects while reducing operator exposure and personal protective equipment (PPE) demands. The field test controller operates from both Android and iOS operating systems for immediate local analysis, results reporting, and automated analysis algorithm enhancements developed through system-wide data analysis.

FIELD LOCATIONS

Hands-Free Scanner(s)

Safely separated from System Operations

On-Site Analysis & Decision Support

Tablet Based

Detailed Data Entry & Situational Awareness Workstation

Advanced Option

SECURE COMMUNICATION

CENTRAL LOCATION

- **Support all field locations**
- **Strategic Data Analysis and Strategic Data Support**
- **Machine Learning / AI for Process & Analysis Improvements**
- **Data Library**

CONCEPT OF OPERATIONS - FIELD LOCATIONS

- Person to be scanned enters Sensor Zone, maintaining safe physical distancing from Operators and other persons to be scanned
- Scanner captures thermal image and sends to Operator Analysis Tablet
- Tablet Operator reviews analysis results and directs person to proceed or to other staff for Follow-On processes
- Data Entry Workstation utilized for additional data collection on scanned individuals
- Field Location data sent to Central Location

CONCEPT OF OPERATIONS - CENTRAL LOCATION

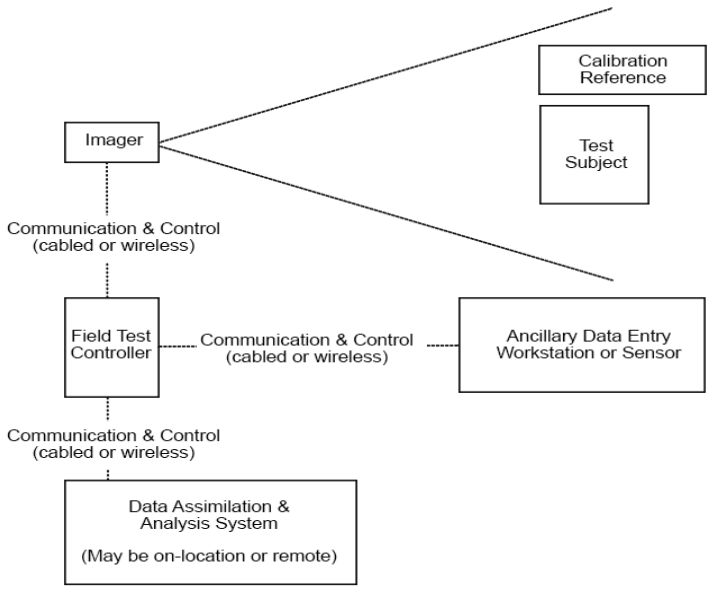
- All field location data is assimilated and analyzed and presented for situational awareness
- Detection algorithm improvements automatically pushed to field sensors
- Data Library used for continuous analysis, trending, ML/AI and Strategic Decision making

The patent pending design:

- Allows less expensive, lower technology imagers to replace high-cost and higher-technology imagers for many applications.
- Maximizes the ability of the camera to deliver its best results by fitting the best response of a given camera (resolution & sensitivity) to the situational needs of the measurement (tuning, measuring, process).
- Utilizes a calibration reference to improve temperature reading accuracy.
- Provides a platform to assimilate image/video data in conjunction with other relevant data, sources, and phenomenologies to improve detection accuracy through field test controller software updates within a context which may be greater than temperature alone; including but not limited to temperature patterns, profiles, environment, and means of presentation.

Based on its ability to integrate data from all field test controllers and an array of complimentary data sources, the COMPAS data assimilation and analysis system provides situational awareness analysis to incident interrogators, responders, and leaders. The field data also populates a data library to support long-term data analysis and research which is used to refine field test controller algorithms for continual system advancement.

The system design was to future-proof your investment allowing for up-to-date deployments for years to come. With this information, incident commanders can not only gain insights into the current state of a pandemic but can also use the COMPAS decision algorithm to determine predicted outcomes based on decisions made in light of the current and future operational pictures.



STEPS
a partnership with
AMERICA

ENTRY ASSESSMENTS

Benjamin M. Butchko

Benjamin is an accomplished senior security executive with proven skill sets in the field of security risk analysis, threat assessments, security consulting, system design, and project planning for national and international building clients. Mr. Butchko's expertise has been applied in diverse markets such as petrochemical, industrial, medical, corporate, and science research industries. His thought leadership and expertise is in demand at security industry events and forums on such subjects as security assessment, strategic planning, design, and deployment. Benjamin Butchko has developed and executed numerous security strategies, CPTED, risk assessment evaluation, system commissioning and operations integration. Clients see him as a key advisor to their short and long term strategic planning. As President and CEO of Butchko Inc. he guides the mission of the company and ensures that the client's sustainable value is paramount in any project we take on. bSMART® and COMPAS inventor.

Walter "Cal" Smith

Cal is an accomplished tactical security officer, security system engineer and US Army National Guard officer. He specializes in protecting high value operations in high-threat situations. He combines practical expertise and experience in field security operations with engineering analysis on sensor systems and integrated security technology. Cal has demonstrated experience in the analysis of security risk, specialized technology countermeasures, explosive ordinance disposal, reliability analysis, sensor characterization, and project management. bSMART® and COMPAS inventor.

Pierre Bourgeix

Pierre has spent 30 years as a global security consultant and innovator through his experience with The Rand Corporation, The US State Department, ADT/Tyco Security, HySecurity, Wallace International, SecureState and BoonEdam. Currently Pierre is the CTO and Founder of ESI Convergent, LLC. Pierre's primary expertise is Physical and Cyber Security Governance and has had years of experience within the physical security arena, including experience working with the US Secret Service, the NSA and the CIA. Projects include a forensic security assessment for Saudi Aramco, and a forward base security assessments in radar detection, geo fencing, and communications testing for the US Navy in Iraq and Kuwait. Pierre also helped the Saudi government implement long-range video surveillance, gate and fence control systems, and ground sensing systems on the Saudi Arabian border. From a strong foundation in the physical security, barrier, gate control industry, Pierre's path has grown to include electronic security, managed services security and finally, the IT and cyber security arena as well. He has spoken at many conferences, manufacturer events and association meetings globally. Pierre is a highly regarded thought leader in the convergence of IT, OT, and Physical Security and is a renowned expert in the integration of converged technology platforms, ranging from large manufacturers to utility companies such as First Energy. He is presently involved in creating security standards for the testing of products, systems, and solutions. Additionally, Pierre is in the process of developing a model that will explain the converged security Kill chain, which will lead to the need for proper predictive analytics across IT, OT, and Physical Security and the development of a converged standard. Pierre's experience includes projects throughout the EU, EMEA and APAC including UAE, Saudi Arabia, Qatar, Kuwait, Iraq, UK, Germany, France, and others. Clients include the Kingdom of Saudi Arabia, The US State Department Security Services, the Rand Corp. The US Navy, Hitachi, First Energy, Meridian, Enel Energy, Space X, Con Ed, Anadarko/ Occidental Petroleum, Exxon, Biogen, AEP, LenelS2, and Carrier UTC. Pierre holds master's degrees in both Behavioral Education and International Business Management, with bachelor's in History and Political Science. He is a member of the US Naval Institute and is fluent in English, French, and Arabic.

ENTRY ASSESSMENTS

Mark Perkins

Mark Perkins' is currently the President and CEO of ESI Convergent, LLC. Mark is an Entry Expert with his most current employment with Boon Edam Inc., as Vice President of Enterprise Security Accounts. His global team is comprised of a group of experts in physical and cyber security entrance solutions focused exclusively on large enterprise accounts. After graduating from the University of Detroit in 1981 with a bachelor's degree in Accounting, Mark worked for several companies, including Litton Industries, Stanley, and Boon Edam Inc. three different times. In between his differing tenures with Boon Edam, Inc., Mark has engaged in multiple start-ups including a construction partnership, children's furniture manufacturing company, a vehicle crash barrier company, a Frac Tank / Vacuum Trailer manufacturing company. Mark spends most of his time leading and training his team, communicating with customers to properly align access control, identity management, and entry solutions into a fully converged-security approach. This includes being a true consultant who looks for where their current entrance security solutions fall short, and then take a big-picture approach to see how Boon Edam security entrances can help with common problems such as piggybacking, mustering, and effective anti-pass back management. Overall, Mark has twenty-seven years of experience in the security industry and was responsible for starting Boon Edam's security products division in the U.S. in the late 90's. Mark has always been a serial entrepreneur, 80/20 facilitator, implementation strategist and most importantly a servant leadership disciple.

Derek Nilsen

Derek Nilsen is the Founder and President of More Better Solutions, LLC a sales and marketing consulting business based in Sandy, UT. Over the past 30 years, Derek has been involved in start-ups and established businesses that span multiple industries including security building entrances, security systems, vehicle barrier systems, oil & gas tanks and equipment, livestock trailers, food processing equipment and nutritional supplements. Back in 1991, Derek was hired by Boon Edam in its US-based operation to develop and grow the U.S. market. With Derek's foresight and leadership, Boon Edam began promoting its line of security revolving doors and portals in the U.S. Today, Boon Edam annually sells thousands of security revolving doors and portals, as well as optical turnstiles, throughout the US and many more throughout the world from its North Carolina based facility; and is the largest Boon Edam subsidiary in the world. Derek has the innate ability to create "channels and markets" and develop growth engines for companies. Examples include security entrances, state-of-the-art electric vehicle barrier systems, vacuum trailers and frac tanks for the oil and gas industry, and for the past year has been helping a manufacturer of nutritional supplements diversify their distribution network and expand into CBD products. Derek received a BS in Manufacturing Engineering from Tufts University in Medford, MA and started his career in the New York City metropolitan area. Derek enjoys hiking, mountain biking, and camping in the mountains of Utah and wherever his travels will take him.

STEPS
a partnership with
AMERICA

HVAC ASSESSMENTS

Rick Perkins, HVAC SME, Retired

Rick Perkins started his temperature controls career in the southeast Michigan area in 1980. Rick has worked for industry leading companies, such as, Johnson Controls, Honeywell, Siemens, and lastly Trane until his retirement in 2017. Rick has worked as a; Field Service Technician, Systems Design Engineer, Project Manager and Estimator. I designed HVAC control systems for laboratories and critical infrastructure environments for the last 25 years. While working for Trane in the Detroit Commercial Sales Office, he worked as a Design Engineer, Project Manager, and Estimator. I was considered the local SME for complex HVAC Systems including Distributed Chilled Water, Steam and HW Boilers, and VAV Air Systems. Rick managed over 50 projects per year with direct responsibility for design compliance of HVAC Equipment and Temperature Controls implementation.

Ed Cihonski, HVAC SME

Ed has over 25 years of experience in the building automation, construction, and energy solutions industries in various capacities, holding positions as Controls Engineer, Turnkey Construction Manager, and Regional Sr. Program Manager. He has experience with a wide array of projects in numerous industrial, commercial, and governmental vertical markets across the US Midwest and South. Ed received his Bachelor's degree in Mechanical Engineering at Purdue University and has achieved Certified Energy Manager certification with the Association of Energy Engineers. Ed is motivated to provide Clients with comprehensive facility solutions focused on improved automation and enhanced energy and operational performance.

SECURITY SYSTEMS

Jim Henry, Integration Specialist SME

James E. Henry (Jim) is currently an independent consultant to Securitas Electronic Security, Inc. (SES). That role includes networking with consultants and manufactures tracking new technologies and major trends to advance "trusted advisor" relationships between SES, clients and industry stakeholders. From June 2018 through November 2019 Jim served as Executive Vice President of Corporate Development for SES. Jim joined SES via the acquisition of the Public Safety and Security division of Kratos Defense & Security Solutions in June 2018. From December 2010 through June 2018 Jim was Executive Vice President (EVP) for Kratos Public Safety & Security Solutions, Inc. (Kratos PSS), a division of Kratos Security and Defense Solutions (KTOS). Jim's title of EVP for Kratos PSS was assumed on December 15, 2010 via the acquisition of Henry Bros. Electronics, Inc. (HBE) by Kratos PSS. From November 2001 through December 15, 2010, Jim was Chairman and CEO of HBE, headquartered first in Saddle Brook, NJ, and then in Fair Lawn, NJ. HBE was sold to a public company in 1986, reacquired by a team led by Jim in 1989, and grown as a private company till Jim took it public in November of 2001. HBE was originally founded as an electronic repair shop in Paramus, NJ in 1950 by John (Jim's father), Hartford and Raymond Henry (the three "Henry Brothers"). Under the ownership of the "Henry Brothers" from 1950 to 1986, HBE grew to have three divisions: Security Systems Integration, Land/Mobile Radio Systems, and Consumer Electronics Sales/Service. Jim joined HBE as an Applications Engineer in June of 1978 after receiving a Bachelor of Science degree in Electrical Engineering from the University of New Hampshire.

Rick Leighton, Sage Integration

Rick Leighton, served as President of of DTS prior to its joining SAGE Integration. With over 25 years experience in client engagement Rick has worked with such industry leaders as ADP, AES and Stanley Security. Rick led DTS in its acquisition and time-tested service of key accounts at Home Depot, T-Mobile, FedEx Ground and Wells Fargo. In addition to his long-standing reputation with enterprise clients, Rick has also led with industry-shifting innovation, including his leadership of SecureVizual, providing a deeply integrated dashboard of Metrics and KPIs for clients' security infrastructure.

VISITOR MANAGEMENT SYSTEMS

Jeff Friedman, Chief Executive Officer, Building Intelligence, Inc.

VIDEO AND ANALYTICS

Sean Grimm, Hitachi

Sean Grimm's most current employment is with Hitachi Vantara as Subject Matter Expert in Smart Spaces and Video Intelligence. Sean was sought after by Hitachi Vantara to create a new IoT sales channel. Due to the demand for Hitachi Vantara IoT solutions, Grimm was moved into a subject matter expert role to facilitate adoption of smart spaces and video intelligence solutions for the sales channel he created as well as end users. For Hitachi Vantara Fiscal Year 2018, Sean was 170% of plan. During Sean's 20-year tenure within the security industry, he has successfully built security sales channel programs for Diebold (from 0 to 1M in 2 years) and Samsung (200k-4M in 2 years). Sean has also held sales individual contributor roles within security manufacturing (Verint) and security integration (Johnson Controls) while being 100%+ of plan every year. Prior to Sean's tenure in the security industry, he held a stadium operations role with the Baltimore Orioles Minor League Affiliate as well as management roles with Major Leagues Sports Franchises (Pittsburgh Pirates and Pittsburgh Steelers). Sean attended Liberty University in Lynchburg, VA with a Bachelor of Arts in Sports Management. Sean currently lives in the Pittsburgh area with his wife and five children. You can often find him travelling with his family, training for his next race or enjoying Pittsburgh sports and cultural events.

GOVERNMENT

Barbara Reeder, President & CEO, Deftec

STEPS
a partnership with
AMERICA

BOARD OF ADVISORS

Physical Security

Cyber Security

Insurance Industry

Medical Industry

Civil Engineer

Legal advisor(s)

Medical Regulation

Political advisor

Analytics advisor

CREDITS

The following individuals participated in the development of the STEPS program.

Listed in alphabetical order

Pierre Bourgeix
Benjamin M. Butchko
Ed Cihonski
Jeff Friedman
Sean Grimm
Jim Henry
Derek Nilsen
Mark Perkins
Rick Perkins
Joe Pinter
David Renaudin
Walter “Cal” Smith

April 2020