Cyber Security and Small Business

27 NOV 2018

Presented by: Darryl Allen, DCIO

CYBER SECURITY AND SMALL BUSINESS Considerations

- Cyber Security support personnel (ISSMs, System Admins, etc.)
  - Cyber Security certified via SANS or others (CISSP, Security Plus GSLC, etc.)
- Team with other companies with similar Cyber interests, if appropriate
- Keep informed of the changing Federal and DOD Cyber landscape
- The threat is real - we see it everyday at NAVAIR and with our Corporate Partners (impacts us all)
- Consider the Cloud for data hosting (e.g. Amazon Web Services)
- Consider alternate Public Key Infrastructure (PKI) capabilities (e.g. external certificate authorities) for data exchange with the DOD
- Have an Incident Response Plan
  - Report Incidents as appropriate

DFARS vs. Cyber Security Plan (CSP)

- DFARS
  - Addresses concerns at a high level
  - Difficult to comprehend intended meaning
  - Results in contractor-generated Systems Security Plan (SSP) / POA&M with no requirement for government approval
  - Allows contractors to be self-regulating / self-policing
- CSP
  - Addresses cybersecurity concerns at a granular level
  - Expectations are well-defined
  - Compliance is approved by the government
  - Compliance is PMA regulated

Basic Elements for Doing Business

- The CSP:
  - Leverages elements that are already commonly in use by contractors who do business with the government resulting in little added cost
    - Personal computers
    - Network connectivity / Internet access
    - Microsoft Office, Adobe
    - Email
  - Requires External Certificate Authority (ECA) PKI encryption
  - For the protection of Controlled Unclassified Information (CUI)
  - Cost associated with procurement of ECA certificates for contractor employees – estimated $100 per employee per year

Effort / Cost of Maintaining CSP/CSIP

- Once a contractor establishes an approved Cybersecurity Implementation Plan (CSIP), it can be leveraged across other entities within the same company
- Costs associated with maintaining the CSIP should be minimal following initial startup costs
- Anticipated on-going CSIP efforts will involve routine bi-yearly reviews to ensure accuracy and continued compliance
- Routine CSIP updates are expected to entail minor changes for addressing evolving threats and associated policy
- Significant CSP updates are expected to be infrequent

Questions / Comments

Backup

CYBER SECURITY AND SMALL BUSINESS
NAVAIR Cyber Stats

- ~32,000 Civilian, Military, Contractor employees that have NMCI seats and require Cyber Security support
- 22 Circuits, NIPR / SIPR / DREN / SDREN
- ~ 800 systems / labs / trainers requiring accreditations
- ~1,000 personnel in the Cyber Security workforce
- Networks fully censored by the Navy's NCDOC and internal CND tool sets