Executive Order (EO) on Improving the Nation’s Cybersecurity

The Executive Order (EO) on Improving the Nation’s Cybersecurity was signed in May and is now in the process of being implemented. The EO is broad ranging in scope, focusing on key areas of vulnerability, including:

- Removing barriers to threat information sharing between government and the private sector
- Modernizing and implementing stronger cybersecurity standards in the federal government
- Improving software supply chain security
- Establishing a cybersecurity safety review board
- Creating a standard playbook for responding to cyber incidents
- Improving detection of cybersecurity incidents on federal government networks
- Improving investigative and remediation capabilities

The principal aim of the EO is to enhance the cybersecurity of government departments and supply chains. However, expect this to have a trickle-down impact on all types of businesses within the private sector, both big and small.

Therefore, small businesses should make themselves aware of the requirements of the EO and determine if they are required to make any changes to remain in compliance, specifically with regards to their vendor relationships.

AN OFFERING IN THE BLUE CYBER SERIES:

NIST SP 800-171 Encryption Requirements Overview & Encryption Primer

Presented by
the DCMA DIBCAC ASSESSMENT TEAM

22 February 2022

#19 in the Blue Cyber Education Series

Distribution Statement A: Coordinated by DCMA.

DEFENSE CONTRACT MANAGEMENT AGENCY

Encryption Requirements in NIST SP 800-171r2

Presented By:

William R. Spence

Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)

February 22, 2022

Agenda

- Confidentiality
- Encryption Basics
- CUI Flow
- Encryption security requirements in NIST SP 800-171
- DIBCAC Assessment Lessons Learned

Confidentiality

- **confidentiality**
  - [44 U.S.C., Sec. 3542] Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Encryption Basics

- **Data Encryption**
  - Data At Rest
  - Data In Use
  - Data In Transit
- **FIPS**
- **VPN/IPsec**
- **Encryption Keys**
- **PKI/Certificates**

Data at rest

- **Data at rest**: By this term we mean data that is not being accessed and is stored on a physical or logical medium. Examples may be files stored on file servers, records in databases, documents on flash drives, hard disks etc.
- Types
  - **Full disk encryption or device – Endpoint, Servers, Storage arrays, Mobile Device Management (MDM)**
  - **File-level encryption – Manual, Digital Right Management**
  - **Database Encryption – Whole database, tables, fields**
  - **Media – USB Drives, DVDs**
  - **Container – MDM**
- CUI Flow
  - Defines where will it be stored
- Cloud Considerations
  - Cloud Service provider (CSP) / Managed Service Provider (MSP) controlled
  - Customer Controlled
- Utilizing physical security is an alternative in some scenarios.
  - Data centers
  - Backups

Data in Use

- **Data in Use**: When it is opened by one or more applications for its treatment or and consumed or accessed by users.
- **Where**
  - Endpoints - entering, processing
  - Servers – receiving, processing
  - IPS/IDS – break and inspect
- **CUI Flow**
  - Defines where it can be processed
- **Utilizing physical security is an alternative in some scenarios**
  - Workspace
  - Datacenter

Data In Transit

- **Data in Transit**: Data that travels through an email, web, collaborative work applications such as Slack or Microsoft Teams, instant messaging, or any type of private or public communication channel. It’s information that is traveling from one point to another.
- **Types**
  - Email
  - Web Services / Cloud Services
  - File servers
  - Physical Media
- **CUI Flow**
  - Defines how the CUI is received, where it us used, and how it is sent
- **Utilizing physical security is an alternative in some scenarios.**
  - Local networks
  - Physical Media

What is FIPS 140-2

- **The Federal Information Processing Standard 140-2 (FIPS 140-2) is a U.S. and Canadian co-sponsored security standard for hardware, software, and firmware solutions.**

- **Cryptographic Module Validation Program | CSRC (nist.gov)**

- **Know the difference**
  - Validated
  - Approved
  - Compliant

- **Plan for the Future**
  - March 22, 2019 - FIPS 140-3 Approved
  - *September 22, 2026 - All FIPS 140-2 certificates are placed on the Historical List*

VPN/Ipsec/HTTPS

- **In Transit**
- **Types**
  - IPSEC is a group of protocols that are used together to set up encrypted connections between devices
  - VPN A virtual private network (VPN) is an encrypted connection between two or more computers,
  - Hypertext Transfer Protocol Secure (HTTPS)The communication protocol is encrypted using Transport Layer Security (TLS)
  - sFTP - SSH File Transfer Protocol is a secure file transfer protocol. It runs over the SSH protocol

- **CUI Flow**
  - Defines how data comes in and goes out of an environment and when a VPN / IPSEC / HTTPS would be used for protection.

Public Key Infrastructure (PKI)/Certificates

- **In Transit / At Rest**
- **Types**
  - Email – Used to protect (Encrypt) data “In Transit”
  - Multi-Factor Authentication – Used to provide access control for “In Use”
  - Endpoint Authentication – Used to provide access for devices “In Use”
  - Endpoint / Device Encryption – Used to Encrypt “At Rest”
  - VPN / IPSEC / HTTPS – Used to Encrypt “In Transit”

DIBCAC Assessment Lessons Learned – Where to start

- ***This is the most important step***
  - What CUI is used
  - How does it come in (In Transit)
  - How is it processed (In Use)
  - How is it stored (At Rest)
  - How does it go out (In Transit)

- **3.1.3 -** Control the flow of CUI in accordance with approved authorizations.
  - *3.1.3[a] information flow control policies are defined.*
  - *3.1.3[b] methods and enforcement mechanisms for controlling the flow of CUI are defined.*
  - *3.1.3[c] designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
  - *3.1.3[d] authorizations for controlling the flow of CUI are defined.*
  - *3.1.3[e] approved authorizations for controlling the flow of CUI are enforced*

CUI Flow

- ***Does your CUI Flow take into account Cybersecurity Capabilities?***
  - *Break and Inspect network packet capabilities*
  - *Cloud based detonation sandbox's*
  - *Anti Malware file submissions*
  - *Incident Response providers taking forensic copies*
- ***Does your CUI Flow account for printing***
  - *Print Servers*
  - *Printer Local Print Job Stores*
  - *Communication Protocols*

Access Control 3.1.13

- **In Transit**
- **3.1.13 -** Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
  - 3.1.13[a] *cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.*
  - 3.1.13[b] *cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.*

- **Common Technologies**
  - HTTPS (TLS)
  - Encrypted RDP
  - VPN / IPSEC
  - SSH

- **Does it need to be FIPS?**
  - Depends on your CUI Flow

- **FAQ**
  - Q72, Q73

Access Control 3.1.17

- **In Transit**
- **3.1.17 -** Protect wireless access using authentication and encryption.
  - 3.1.17[a] *wireless access to the system is protected using authentication.*
  - 3.1.17[b] *wireless access to the system is protected using encryption.*

- **Common Technologies**
  - Wi-Fi Protected Access II (WPA2) (pre-shared key (PSK) , PKI)
  - Wi-Fi Protected Access 3 (WPA3) (Simultaneous Authentication of Equals (SAE), PKI)

- **Does it need to be FIPS?**
  - Depends on your CUI Flow

- **FAQ**
  - Q72, Q73

Access Control 3.1.19

- **In Transit / At Rest / In Use**
- **3.1.19 -** Encrypt CUI on mobile devices and mobile computing platforms.
  - 3.1.19[a] *mobile devices and mobile computing platforms that process, store, or transmit CUI are identified.*
  - 3.1.19[b] *encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.*

- **Common Technologies**
  - PKI
  - Device or Container Encryption
  - MDM

- **Does it need to be FIPS?**
  - Yes CUI is involved

- **FAQ**
  - Q72

Identification and Authentication 3.5.10

- **In Transit / At Rest**
- **3.5.10 -** Store and transmit only cryptographically-protected passwords.
  - 3.5.10[a] *passwords are cryptographically protected in storage.*
  - 3.5.10[b] *passwords are cryptographically protected in transit.*

- **Common Technologies**
  - Kerberos / IPSEC
  - Password Vaults
  - PKI
  - Password protected file

- **Does it need to be FIPS?**
  - No, the passwords are not CUI

- **FAQ**
  - Q88

Media Protection 3.8.6

- **In Transit / At Rest**
- **3.8.6 -** Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

- **Common Technologies**
  - Encrypted Media
    - USB / DVD
  - Physical Controls

System and Communications Protection 3.13.4

- **In Use**
- **3.13.4 -** Prevent unauthorized and unintended information transfer via shared system resources.

- **Common Technologies**
  - Encryption during processing
  - Encrypted tables

- **Does it need to be FIPS?**
  - Depends on your CUI Flow

- **Cloud Concerns**
  - What are the shared system resources?

System and Communications Protection 3.13.8

- **In Transit**
- **3.13.8-** Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
  - 3.13.8[a] *cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.*
  - 3.13.8[b] *alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.*
  - 3.13.8[c] *either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.*

- **CUI Flow**
  - Defines what transportation technologies will have to be FIPS Validates

- **Common Technologies**
  - HTTPS (TLS)
  - PKI
  - Physical Controls

- **Does it need to be FIPS?**
  - Yes CUI is involved

- **FAQ**
  - Q72, Q101, Q102

System and Communications Protection 3.13.10

- **In Transit**
- **3.13.10 -** Establish and manage cryptographic keys for cryptography employed in organizational systems.
  - 3.13.10[a] *cryptographic keys are established whenever cryptography is employed.*
  - 3.13.10[b] *cryptographic keys are managed whenever cryptography is employed.*

- **Common Technologies**
  - Endpoint / Device Encryption Managers
  - PKI (Server HTTPS, MFA, Device Auth)
  - Commercial Certificate Providers
  - DRM

- **Cloud Concerns**
  - Managing Keys for cloud Instance

System and Communications Protection 3.13.11

- **In Transit / At Rest**
- **3.13.11 -** Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

- Cryptographic Module Validation Program | CSRC (nist.gov)

- **CUI Flow**
  - Defines what will have to be FIPS Validates

- **Common Technologies**
  - Endpoint / Device Encryption
  - PKI (Server HTTPS, MFA, Device Auth)
  - File Encryption (DRM, Manual)
  - Removable Media

- **Know the difference**
  - Validated
  - Approved
  - Compliant

- **FAQ**
  - Q72

System and Communications Protection 3.13.16

- **At Rest**
- **3.13.16 -** Protect the confidentiality of CUI at rest.

- **CUI Flow**
  - Defines what will have to be FIPS Validates

- **Common Technologies**
  - Endpoint / Device Encryption
  - File Encryption (DRM, Manual)
  - Removable Media
  - Backup Media
  - Physical Protections

Questions

SUPPLEMENTAL

DFARS FAQs

DoD Procurement Toolbox Cybersecurity FAQS

- **Q7: Our Company has outsourced its IT support and systems to a third-party contractor. Are we still responsible for complying with DFARS clause 252.204-7012 and implementing NIST SP 800-171?"**
  - **A7:** Outsourcing your IT to another company does not transfer your DFARS clause 252.204-7012 responsibilities or implementation of NIST SP 800-171 requirements. Your company is responsible and accountable for meeting the contractual obligations with the Government as per the contract. The key to successfully demonstrating compliance with DFARS clause 252.204-7012 and NIST SP 800-171 is having a well written contract with the third-party that describes your requirements, and includes deliverables that meet or exceed requirements to protect DoD CUI. If your IT service support is deemed to be less than or non-compliant with the contract, the company contracting with DoD is ultimately responsible.

- **Q72: Security Requirements 3.1.13, 3.1.17, 3.1.19, 3.13.8, and 3.13.11 – Do all of the 171 security requirements for cryptography have to be FIPS validated, and if so, what does that mean? If the algorithm is FIPS approved, is that sufficient?**
  - A72: Yes, all the NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI (or in this case covered defense information) must use FIPS-validated cryptography, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at http://csrc.nist.gov/groups/STM/cmvp/ and http://csrc.nist.gov/groups/STM/cmvp/validation.html. When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI (or in this case covered defense information). Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS validated cryptography is required whenever the encryption is required to protect covered defense information in accordance with NIST SP 800-171 or by another contract provision. Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS validated cryptography.

DFARS FAQs

DoD Procurement Toolbox Cybersecurity FAQS

- **Q59: How will the DoD account for the fact that compliance with NIST SP 800-171 is an iterative and ongoing process? The DFARS clause imposing NIST SP 800-171 requires that the entire system be in 100% compliance all the time, a condition that in practice (in industry or Government) is almost never the case.**
  For example:

  - It is not possible to apply session lock or termination (Requirements 3.1.10/11) to certain computers (e.g., in a production line or medical life-support machines).

  - Applying a necessary security patch can "invalidate" FIPS validated encryption (Requirement 3.13.11) since the encryption module "with the patch" has not been validated by NIST.

  - Segments of an information system may be incapable of meeting certain requirements, such as correcting flaws/patching vulnerabilities (Requirement 3.14.1) without disrupting production/operations that may be critical to the customer.

  - How should a contractor deal with situations such as these?

  - A59: The requirement at DFARS clause 252.204-7012 (b)(2)(i) to implement, at a minimum, the security requirements in NIST SP 800-171, is not intended to imply that there will not be situations where elements of the NIST SP 800-171 requirements cannot practically be applied, or when events result in short- or long-term issues that have to be addressed by assessing risk and applying mitigations. The rule allows a contractor to identify situations in which a required control might not be necessary or an alternative but equally effective control can be used, and the DoD CIO will determine whether the identified variance is permitted, in accordance with DFARS provision 252.204-7008(c)(2)(i) and (ii) and DFARS clause 252.204-7012(b)(2)(ii).
    In addition, the dynamic nature of cybersecurity threats and vulnerabilities is recognized within the NIST SP 800-171. The contractor should address situations such as those listed above in accordance with the NIST SP 800-171 security requirements that follow:

    - 3.11.1, Risk Assessment: Requires the contractor to periodically assess the risk associated with operating information systems processing CUI;

    - 3.12.1, Security Assessment: Requires the contractor to periodically assess the effectiveness of organizational information systems security controls;

    - 3.12.2, Security Assessment: Requires the contractor to "develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;"

    - 3.12.3, Security Assessment: Monitor security controls in an ongoing basis to ensure the continued effectiveness of the controls;" and

    - 3.12.4, System security plan: Requires the contractor to "develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems."

    The contractor should address issues, security requirement implementations in progress, special circumstances/enduring exceptions, and any individual, isolated or temporary deficiencies through "plans of action" (as described in security requirement 3.12.2) and in the system security plan (as described in security requirement 3.12.4). As provided at 252.204-7012 (b)(3), a system security plan may be used to describe how the system security protections are implemented, any exceptions to the requirements to accommodate special circumstances (e.g., medical devices), any individual, isolated or temporary deficiencies based on an assessed risk or vulnerability per NIST SP 800-171 security requirements 3.11.1, 3.12.1, and 3.12.3, and plans of action as provided by security requirement 3.12.2, to correct deficiencies and reduce or eliminate vulnerabilities identified through the assessment process. Elements of the security plan may be included with the contractor's technical proposal (and may subsequently be incorporated as part of the contract). These also may inform a discussion of risk between the contractor and requiring activity/program office.

DFARS FAQs 3.5.10

DoD Procurement Toolbox Cybersecurity FAQS

- **Q88: Security Requirement 3.5.10 – Store and transmit only encrypted representations of passwords (in Revision 1, “encrypted representations of passwords” is changed to “cryptographically-protected password).” Is a HASH considered an “encrypted representation” of a password or a cryptographically-protected password?**
    - A88: Yes, the Supplemental Guidance in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, for the related security control IA-5(1) notes that “Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords.” Best practice would add a unique “salt” to the password before hashing. This description applies to the use

DFARS FAQs 3.13.8

DoD Procurement Toolbox Cybersecurity FAQS

- **Q101: Security Requirement 3.13.8 – When implementing the requirement to "Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards," is encryption required for a Multiprotocol Label Switching (MPLS) private network (thus an extension of a local network) but it is multi-tenant protected by VLANs?**
  - A101: Encryption, though preferred, is not required if using common-carrier provided MPLS, as the MPLS separation provides sufficient protection without encryption.
- **Q102: Security Requirement 3.13.8 – Can Transport Layer Security (TLS) protocol be used to protect CUI during transmission over the Internet?**
  - A102: Yes, TLS can be used. The current version of TLS (TLS 1.2) is preferred. If earlier versions must be used to interact with certain organizations, the servers shall not support Secure Sockets Layer (SSL) version 3.0 or earlier. The cryptographic module used by the server and client must be a FIPS 140-validated cryptographic module. All cryptographic algorithms that are included in the configured cipher suites must be within the scope of the validation, as well as the random number generator. For further information see NIST SP 800-52, Rev 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, April 2014.
- **Q103: Regarding security requirement 3.13.8– How is CUI to be protected when transmitted over Common Carrier telecommunications lines/Plain Old Telephone Service (POTS)?**
  - A103: Common Carrier telecommunications circuits or Plain Old Telephone Service (POTS) would not normally be considered part of the information system processing CUI. Data traversing Common Carrier systems should be separately encrypted per 3.13.8. Contracts with Common Carriers to provide telecommunications services may include DFARS clause 252.204-7012, but should not be interpreted to imply the Common Carrier telecommunications systems themselves have to meet the DFARS requirements. Data transmission of CUI transmitted over standard telephone dial-up service (POTS) similarly should be separately encrypted as no protection is expected to be provided by the telephone system. Voice communication of CUI over the telephone is not addressed by NIST SP 800-171 or by DFARS clause 252.204-7012.

DFARS FAQs 3.13.16

DoD Procurement Toolbox Cybersecurity FAQS

- **Q105: Security Requirement 3.13.16 – Protect the Confidentiality of CUI at rest. Can CUI be stored at rest in any non-mobile device or data center, unencrypted, as long as it is protected by other approved logical or physical methods?**
    - A105: Yes, the mapped NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, control (SC-8), notes that this requirement is to protect the confidentiality of CUI information at rest when it is located on storage devices as specific components of information systems and that "organizations may employ different mechanisms to achieve confidentiality protection, including the use of

References

- DOD CMMC Website https://www.acq.osd.mil/cmmc/
- NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf
- NIST MEP Cybersecurity Self-Assessment Handbook https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf
- SPRS NIST SP 800-171 Quick Entry Guide https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf
- NIST CUI SSP Template https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-1/final/documents/CUI-SSP-Template-final.docx
- NIST CUI Plan of Action Template https://csrc.nist.gov/CSRC/media//Publications/sp/800-171/rev-1/final/documents/CUI-Plan-of-Action-Template-final.docx
- Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/)
- NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf