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
Policies and Procedures
An Overview

15 Sep 2021
#17 in the Blue Cyber Education Series
NIST SP 800-171 Policies And Procedures
An Overview

Presented By:
Ms. Mia Hazelgrove & Mr. Patrick Wicker
DCMA DIBCAC
December 14th, 2021

Controlled by: DCMA
Controlled by: DIBCAC
CUI Category: Uncontrolled Unclassified Information
Distribution/Dissemination Control: N/A
POC: dcma.lee.hq.mbx.dibcac-scheduling-inbox@mail.mil

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.
### NIST 800-171 IN A NUTSHELL

<table>
<thead>
<tr>
<th>AC</th>
<th>AT</th>
<th>AU</th>
<th>CM</th>
<th>IA</th>
<th>IR</th>
<th>MT</th>
<th>MP</th>
<th>PS</th>
<th>PE</th>
<th>RA</th>
<th>CA</th>
<th>SC</th>
<th>SI</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1</td>
<td>3.2.1</td>
<td>3.3.1</td>
<td>3.4.1</td>
<td>3.5.1</td>
<td>3.6.1</td>
<td>3.7.1</td>
<td>3.8.1</td>
<td>3.9.1</td>
<td>3.10.1</td>
<td>3.11.1</td>
<td>3.12.1</td>
<td>3.13.1</td>
<td>3.14.1</td>
</tr>
<tr>
<td>3.1.2</td>
<td>3.2.2</td>
<td>3.3.2</td>
<td>3.4.2</td>
<td>3.5.2</td>
<td>3.6.2</td>
<td>3.7.2</td>
<td>3.8.2</td>
<td>3.9.2</td>
<td>3.10.2</td>
<td>3.11.2</td>
<td>3.12.2</td>
<td>3.13.2</td>
<td>3.14.2</td>
</tr>
<tr>
<td>3.1.3</td>
<td>3.2.3</td>
<td>3.3.3</td>
<td>3.4.3</td>
<td>3.5.3</td>
<td>3.6.3</td>
<td>3.7.3</td>
<td>3.8.3</td>
<td>3.9.3</td>
<td>3.10.3</td>
<td>3.11.3</td>
<td>3.12.3</td>
<td>3.13.3</td>
<td>3.14.3</td>
</tr>
<tr>
<td>3.1.4</td>
<td>3.2.4</td>
<td>3.3.4</td>
<td>3.4.4</td>
<td>3.5.4</td>
<td>3.6.4</td>
<td>3.7.4</td>
<td>3.8.4</td>
<td>3.9.4</td>
<td>3.10.4</td>
<td>3.11.4</td>
<td>3.12.4</td>
<td>3.13.4</td>
<td>3.14.4</td>
</tr>
<tr>
<td>3.1.5</td>
<td>3.2.5</td>
<td>3.3.5</td>
<td>3.4.5</td>
<td>3.5.5</td>
<td>3.6.5</td>
<td>3.7.5</td>
<td>3.8.5</td>
<td>3.9.5</td>
<td>3.10.5</td>
<td>3.11.5</td>
<td>3.12.5</td>
<td>3.13.5</td>
<td>3.14.5</td>
</tr>
<tr>
<td>3.1.6</td>
<td>3.2.6</td>
<td>3.3.6</td>
<td>3.4.6</td>
<td>3.5.6</td>
<td>3.6.6</td>
<td>3.7.6</td>
<td>3.8.6</td>
<td>3.9.6</td>
<td>3.10.6</td>
<td>3.11.6</td>
<td>3.12.6</td>
<td>3.13.6</td>
<td>3.14.6</td>
</tr>
<tr>
<td>3.1.7</td>
<td>3.2.7</td>
<td>3.3.7</td>
<td>3.4.7</td>
<td>3.5.7</td>
<td>3.6.7</td>
<td>3.7.7</td>
<td>3.8.7</td>
<td>3.9.7</td>
<td>3.10.7</td>
<td>3.11.7</td>
<td>3.12.7</td>
<td>3.13.7</td>
<td>3.14.7</td>
</tr>
<tr>
<td>3.1.8</td>
<td>3.2.8</td>
<td>3.3.8</td>
<td>3.4.8</td>
<td>3.5.8</td>
<td>3.6.8</td>
<td>3.7.8</td>
<td>3.8.8</td>
<td>3.9.8</td>
<td>3.10.8</td>
<td>3.11.8</td>
<td>3.12.8</td>
<td>3.13.8</td>
<td>3.14.8</td>
</tr>
<tr>
<td>3.1.9</td>
<td>3.2.9</td>
<td>3.3.9</td>
<td>3.4.9</td>
<td>3.5.9</td>
<td>3.6.9</td>
<td>3.7.9</td>
<td>3.8.9</td>
<td>3.9.9</td>
<td>3.10.9</td>
<td>3.11.9</td>
<td>3.12.9</td>
<td>3.13.9</td>
<td>3.14.9</td>
</tr>
<tr>
<td>3.1.10</td>
<td>3.2.10</td>
<td>3.3.10</td>
<td>3.4.10</td>
<td>3.5.10</td>
<td>3.6.10</td>
<td>3.7.10</td>
<td>3.8.10</td>
<td>3.9.10</td>
<td>3.10.10</td>
<td>3.11.10</td>
<td>3.12.10</td>
<td>3.13.10</td>
<td>3.14.10</td>
</tr>
<tr>
<td>3.1.11</td>
<td>3.2.11</td>
<td>3.3.11</td>
<td>3.4.11</td>
<td>3.5.11</td>
<td>3.6.11</td>
<td>3.7.11</td>
<td>3.8.11</td>
<td>3.9.11</td>
<td>3.10.11</td>
<td>3.11.11</td>
<td>3.12.11</td>
<td>3.13.11</td>
<td>3.14.11</td>
</tr>
<tr>
<td>3.1.15</td>
<td>3.2.15</td>
<td>3.3.15</td>
<td>3.4.15</td>
<td>3.5.15</td>
<td>3.6.15</td>
<td>3.7.15</td>
<td>3.8.15</td>
<td>3.9.15</td>
<td>3.10.15</td>
<td>3.11.15</td>
<td>3.12.15</td>
<td>3.13.15</td>
<td>3.14.15</td>
</tr>
<tr>
<td>3.1.16</td>
<td>3.2.16</td>
<td>3.3.16</td>
<td>3.4.16</td>
<td>3.5.16</td>
<td>3.6.16</td>
<td>3.7.16</td>
<td>3.8.16</td>
<td>3.9.16</td>
<td>3.10.16</td>
<td>3.11.16</td>
<td>3.12.16</td>
<td>3.13.16</td>
<td>3.14.16</td>
</tr>
</tbody>
</table>

- **AC**: Administrative (e.g., policies, standards & procedures)
- **AT**: Assigned Tasks To Cybersecurity Personnel
- **AU**: Assigned Tasks To IT Personnel
- **CM**: Technical Configurations (e.g., security settings)
- **IA**: Assigned Tasks To Application/Asset/Process Owner
- **IR**: Software Solution
- **MT**: Configuration or Software Solution
- **MP**: Hardware Solution
- **PS**: Configuration or Software or Hardware or Outsourced Solution
- **PE**: Software or Hardware Solution

---

**DISTRIBUTION STATEMENT A.** Approved for public release: distribution unlimited.
The Policies and Procedures which you will write for the implementation of NIST SP 800-171 will depend on the data, data flows and Information System architecture of your business.

• In other words, you must do this **SCOPING** work first

• See the Blue Cyber Presentation “Getting Started with NIST SP 800-171”
• It starts with a System Security Plan (SSP) rule #1
  - NIST SP 800-18 is a good reference
  - NIST SP 800-171 (3.12)

• What is “in scope”? See rule #1
  - Enterprise boundary (logical/physical/cloud/ etc..) (3.1, 3.4, 3.5, 3.6, 3.11, 3.13, 3.14)
  - Wireless/mobile/cloud? (3.1, 3.3, 3.4, 3.5, 3.7, 3.9, 3.10, 3.11, 3.13, 3.14)
    • CAAS/virtual enterprise/ etc...
  - Standalone systems (does it process, transmit, or store CUI?)
    • enduring exception?
  - Know what is in the enterprise
    • HW/SW/FW etc... (3.4, 3.5, 3.6, 3.7, 3.11, 3.13, 3.14)
    • Not Applicable? Temporary Deficiency?
Top-down
- Legal
- Regulatory
- Business/Financial
- Executive
- Administrative

Bottom-up
- NIST SP 800-171

Policy Types:
- Administrative
- Technical
- Physical

Controls:
- Administrative
- Technical
- Physical
• Implement security requirements identified in NIST SP 800-171
  - 3.12.4 – “Develop, document and periodically update system security plans…”

• Rapidly (within 72 hours) report cyber incidents
  - 3.6.1 – “Establish an operational incident response handling capability…”

• Submit malicious software to DC3 in accordance with instructions provided by
  DC3 or the Contracting Officer

• Preserve/protect affected media for 90 days
  - 3.3.1 – “Create and retain system audit logs and records to the extent needed…”

• Flow down DFARS clause requirements to subcontractors
Purpose:

The purpose of the policy should be stated clearly and in plain language. If a policy is not written in plain language, employees may not understand it. If an employee can not understand a policy, they may not follow it. If the policy is long-winded or addresses many different topics, then the policy has been diluted and the message trying to be conveyed will lose its meaning. A policy that is short and clear is easily memorable by an employee.

Scope:

The scope of a policy is used to restrict the rules defined by the policy to a specific application or set of circumstances. A well-defined scope will identify what the policy is applied against. Additionally, the scope will identify the intended audience of the policy. A policy should be broad enough that it does not need to change frequently.
Roles and Responsibilities:

- Assignment of the activities covered by the policy are defined (responsibilities, authority, ownership, i.e. RACI)
- Separates policy ownership from policy execution
- Establishes or directs establishment of procedures to carry out and meet the intent of the policy

References:

- Regulatory
- Statutory
- Guides
- Standards
Leadership Buy-in:
- Leadership should endorse the policy
- Leadership should ensure the policy is available to employees and disseminated appropriately.
- Leadership should appoint a champion to the policy
- Leadership should ensure the policy is reviewed and updated periodically

Defines the Objectives:
- What are you trying to achieve?
- What is the desired outcome?
- Is there a specific target?
Procedures are implanted to enact governance to ensure the objectives of policy are met. Procedures should be:

- Documented
- Repeatable
- Detailed to a sufficient level that minimizes variation
- Specific to activities required to carry out the tasks
- Reviewed and updated periodically
NIST SP 800-171, Appendix E:

**TAILORING CRITERIA**

This appendix provides a list of the security controls in the NIST SP 800-53 moderate baseline, one of the sources along with the CBP in PGI 200, used to develop the CUI security requirements described in Chapter Three. Tables E-1 through E-17 contain the specific tailoring actions that have been carried out on the controls in accordance with the tailoring criteria established by NIST and NMA. The tailoring actions facilitated the development of the CUI derived security requirements which supplement the basic security requirements. There are three primary criteria for eliminating a security control or control enhancement from the baseline, including:

- The control or control enhancement is uniquely federal (i.e., primarily the responsibility of the federal government);
- The control or control enhancement is not directly related to protecting the confidentiality of CUI;

and

- The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification.

The following symbols in Table E are used in Tables E-1 through E-17 to specify the tailoring actions taken during the tailoring process, and when no tailoring actions were required.

**TABLE E-1: TAILORING ACTIONS FOR ACCESS CONTROLS**

<table>
<thead>
<tr>
<th>NIST SP 800-53 MODERATE Baseline SECURITY CONTROLS</th>
<th>TAILORING ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-1 Access Control Policy and Procedures</td>
<td>NFO</td>
</tr>
<tr>
<td>AC-2 Account Management</td>
<td>LOI</td>
</tr>
<tr>
<td>AC-2(1) ACCOUNT MANAGEMENT</td>
<td>AUTOMATED SYSTEM ACCOUNT MANAGEMENT</td>
</tr>
<tr>
<td>AC-2(2) ACCOUNT MANAGEMENT</td>
<td>REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS</td>
</tr>
<tr>
<td>AC-2(3) ACCOUNT MANAGEMENT</td>
<td>DISABLE INACTIVE ACCOUNTS</td>
</tr>
<tr>
<td>AC-2(4) ACCOUNT MANAGEMENT</td>
<td>AUTOMATED AUDIT ACTIONS</td>
</tr>
</tbody>
</table>
AC-1 POLICY AND PROCEDURES

Family: AC - ACCESS CONTROL

Security Baseline:
- Low: AC-1
- Moderate: AC-1
- High: AC-1

Privacy Baseline: AC-1

Control

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that:
      a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:
   1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
   2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.
### TABLE D-1: MAPPING ACCESS CONTROL REQUIREMENTS TO CONTROLS

<table>
<thead>
<tr>
<th>SECURITY REQUIREMENTS</th>
<th>NIST SP 800-53 Relevant Security Controls</th>
<th>ISO/IEC 27001 Relevant Security Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3.1 ACCESS CONTROL</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Basic Security Requirements</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).</td>
<td>AC-2 Account Management</td>
<td>A.9.2.1 User registration and de-registration</td>
</tr>
<tr>
<td>3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.</td>
<td></td>
<td>A.9.2.2 User access provisioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.9.2.3 Management of privileged access rights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.9.2.5 Review of user access rights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.9.2.6 Removal or adjustment of access rights</td>
</tr>
<tr>
<td>AC-3 Access Enforcement</td>
<td></td>
<td>A.6.2.2 Teleworking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.2.1.2 Access to networks and network services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.3.4.1 Information access restriction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.2.4.4 Use of privileged utility programs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.3.4.5 Access control to program source code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.13.1.1 Network controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.14.1.2 Securing application services on public networks</td>
</tr>
</tbody>
</table>

**DISTRIBUTION STATEMENT A.** Approved for public release: distribution unlimited.
• Companion document to NIST SP 800-171r2
• Method for performing DIBCAC CUI assessments
• 320 objectives covering 110 security requirements
• DIBCAC assesses down to the **objective** level
• Many objectives describe potential objects (policies) to examine and elements to be **defined** or **documented**
3.1.3 SECURITY REQUIREMENT
Control the flow of CUI in accordance with approved authorizations.

<table>
<thead>
<tr>
<th>ASSESSMENT OBJECTIVE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine if:</td>
<td></td>
</tr>
</tbody>
</table>

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.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine: [SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records].

Interview: [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers].

Test: [SELECT FROM: Mechanisms implementing information flow enforcement policy].
- Assist small manufacturers in preparing for assessment
- Mirrors SP 800-171A
- Self-Assessment Handbook for assessing NIST SP 800-171
- Provides step-by-step guide on assessment methods
  - Examine – Where to Look
  - Interview – Who to Talk To
  - Test – How to Test
- Appendix A – Suggested Plans, Policies, Procedures
3.1.6 Control the flow of CUI in accordance with approved authorizations.

- Do you have architectural solutions to control the flow of systems data?
- Yes, but it's not at the top level. Are there alternatives?
- Yes, but it's not at the top level. Are there alternatives?

**Additional Information:**

The solutions must include firewall, proxy, encryption, and other security technologies. Information flow control regulates how information can travel within an information system and between information systems. An objective is often to allow access to the information without explicit regard to subsequent access to that information.

Examples of flow control solutions include:

- Keeping remote-controlled information flows being transmitted as the clear is the response.
- Blocking outside traffic that claims to be from within the organization.
- Restricting web requests to the internet that are not from the external web proxy server, and
- Limiting information access between organizations based on data structures and attributes.

Transmitting information between information systems representing different security domains with different security policies introduces a risk that each transmission violates one or more domain security policies. In such situations, information sources/sources provide guidance and technical policy enforcement points between interconnected systems. The company may consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example:

- Providing information transfer between interconnected systems (i.e., aligning access controls),
- Employing hardware mechanisms to enforce one-way information flow, and
- Implementing necessary security mechanisms to mitigate security weaknesses and security policy.

Companies commonly deploy information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, subnets, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and the information path. Enforcement occurs, for example, in boundary protection devices (e.g., firewalls, proxies, guards, and access control). Information that employs multiple sets of enforcement criteria may require one or more security measures or one document (characterization). Companies may also consider the interrelatedness of flow policy enforcement mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

Where to Look:

- Access control policy
- Information flow control policies
- Procedures addressing information flow enforcement
- Information system design and documentation
- Information system configuration settings and associated documentation
- Information system baseline configuration
- List of information flow authorizations
- Information system audit logs
- Other relevant documents or records

Who to Talk to:

- System/Network Administrators
- Employees with information security responsibilities
- System developers
- Technical support staff

Performance Test exciting
- Automated mechanisms for implementing information flow enforcement policy
3.1.2 - Limit system access to the types of transactions and functions that authorized users are permitted to execute
   3.1.2[a] - the types of transactions and functions that authorized users are permitted to execute are defined
   (acceptable use policy, remote access policy, privileged user agreement, etc...)

3.1.3 Control the flow of CUI in accordance with approved authorizations
   3.1.3[a] information flow control policies are defined (email handling policy [safe URL, disallowed attachments, attachment size, phishing reporting], internet use policy [smart filters, blocked categories], removable media policy [restrictions, authorized exceptions, exception process], etc...)

3.1.21 Limit use of portable storage devices on external systems
   3.1.21[b] - limits on the use of portable storage devices containing CUI on external systems are defined

3.1.22 Control CUI posted or processed on publicly accessible systems
   3.1.22[c] - a review process is in place prior to posting of any content to publicly accessible systems
   3.1.22[e] - mechanisms are in place to remove and address improper posting of CUI (spillage procedure)
3.1.16 Authorize wireless access prior to allowing such connections

- If, the company does NOT allow wireless with documented policy (administrative control)
- Or if the company does NOT allow wireless with additional tool-based policy (technical control)
- Or if the company does NOT allow wireless devices on premise (physical control)
- Then, include those policy languages to the overall policy (SSP)
- Per guidance, it could be considered "satisfied" in the assessment *
  - *verification by assessing entities may want to see the policy
  - *And, or see the technical controls in place
3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles

3.4.1[b] the baseline configuration includes hardware, software, firmware, and documentation.

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems

3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software

3.4.9 Control and monitor user-installed software
3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services

- 3.4.7[a] essential programs are defined. (documentation: administrative control policy)
- 3.4.7[b] the use of nonessential programs is defined. (documentation: administrative control policy)
- 3.4.7[c] the use of nonessential programs is restricted, disabled, or prevented as defined. (technical control and policy)
3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application

3.12.1[a] - the frequency of security control assessments is defined (information security policy, continuous monitoring policy, etc.)

3.12.4 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

3.12.4[g] - the frequency to update the system security plan is defined (SSP review frequency, revision history)
3.14.1 Identify, report, and correct system flaws in a timely manner
   3.14.1[a] - the time within which to identify system flaws is specified (patch management)
   3.14.1[c] - the time within which to report system flaws is specified (patch management)
   3.14.1[e] - the time within which to correct system flaws is specified (patch management)

3.14.7 Monitor system security alerts and advisories and take action in response
   3.14.7[a] - authorized use of the system is defined (acceptable use policy, unacceptable use)
3.14.1 Identify, report, and correct system flaws in a timely manner

3.14.1[a] the time within which to identify system flaws is specified. (administrative control policy, and may apply to technical control policies)

3.14.1[d] system flaws are reported within the specified time frame. (technical control procedures followed in accordance with administrative and technical control policy)
• Multi-factor authentication not implemented completely
• Not using Federal Information Processing Standards (FIPS) 140-2 VALIDATED cryptography for data in transit and at rest protections
• Poorly written and detailed System Security Plans
• Network Segregation (see Rule #1)
• Configuration management, user installed software lack of policy and enforcement to not allow it
• Know where CUI is processed, transmitted, and stored within your organization

• Maintain a network topology that accompanies your system security plan and describes CUI flow in your organization

• Trace security architecture (policies, processes, appliances, tools) to security requirements addressed in NIST SP 800-171
References

- NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1

- NIST MEP Cybersecurity Self-Assessment Handbook

- SPRS NIST SP 800-171 Quick Entry Guide

- NIST CUI SSP Template

- NIST CUI Plan of Action Template

- Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil)

- NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information
Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.

- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/Organizations/CISO-Homepage/Small-Business-Cybersecurity-Information/

- Please provide questions, feedback or if you just want to talk about your cybersecurity/data protection questions to Kelley.Kiernan@us.af.mil

  - Daily Office Hours for answering/researching your questions about DAF Small Business cybersecurity and data protection!

  - Every Tuesday, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything. Register in advance for this Zoom Webinar: https://www.zoomgov.com/webinar/register/WN_CHsGAoWXTJSU5cDvEmQQHQ