Federal Contractor Security:
NIST Special Publication (SP) 800-171 Series and High Value Asset Protection

Information Security and Privacy Advisory Board
August 8, 2019

Victoria Yan Pillitteri
Computer Security Division
NIST

Alan McClelland
HVA Program Manager
CISA DHS
Federal Contractor Security: NIST Special Publication 800-171 Series and High Value Asset Protection

• **Overview** of the NIST Special Publication (SP) 800-171, SP 800-171A, and Draft SP 800-171B

• Relationship between the **High Value Assets (HVA) Program** and SP 800-171B

• **Next steps** and ongoing interagency collaboration

• **Questions** and contact information
NIST Special Publication 800-171, Revision 1
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Published: December 2016 [Updated June 2018]

Purpose: Provide federal agencies a set of recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations.

*Draft NIST SP 800-171, Revision 2 was also released for public comment in June 2019; there were no substantive changes to the security requirements.

For more information about Protecting Controlled Unclassified Information, NIST, DoD, and NARA, held a workshop in October 2018. Workshop presentations and recordings are available at: go.usa.gov/xUkXQ
NIST Special Publication 800-171A
Assessing Security Requirements for Controlled Unclassified Information

Published: June 2018

Purpose: Provides federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in NIST Special Publication 800-171.

Draft NIST Special Publication 800-171B
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets

Draft Published: June 2019 [Public Comment Period Closed August 2, 2019]

Purpose: Enhanced security requirements for protecting CUI in nonfederal systems and organizations where that information runs a higher than usual risk of exposure (e.g., part of a critical program or high value asset (HVA)). The enhanced security requirements:

- are implemented in addition to the basic and derived requirements in NIST SP 800-171;
- apply only to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components when the designated CUI is contained in a critical program or HVA.
- are only applicable for a nonfederal system or organization when mandated by a federal agency in a contract, grant, or other agreement.
Draft NIST Special Publication 800-171B
Assessing Security Requirements for Controlled Unclassified Information

SP 800-171B Security Requirement Families

34 enhanced security requirements

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Awareness &amp; Training</th>
<th>Audit and Accountability*</th>
<th>Configuration Management</th>
<th>Identification &amp; Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 enhanced security reqs</td>
<td>2 enhanced security reqs</td>
<td></td>
<td>3 enhanced security reqs</td>
<td>3 enhanced security reqs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incident Response</th>
<th>Maintenance*</th>
<th>Media Protection*</th>
<th>Personnel Security</th>
<th>Physical Protection*</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 enhanced security reqs</td>
<td></td>
<td></td>
<td>3 enhanced security reqs</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Assessment</th>
<th>Security Assessment</th>
<th>System &amp; Communications Protection</th>
<th>System &amp; Information Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 enhanced security reqs</td>
<td>1 enhanced security req</td>
<td>4 enhanced security reqs</td>
<td>6 enhanced security reqs</td>
</tr>
</tbody>
</table>

*Indicates no enhanced security requirements for this family

Examples of Enhanced Security Requirements

3.1.1e: Employ dual authorization to execute critical or sensitive system and organizational operations.

3.4.1e: Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.

3.6.1e: Establish and maintain a full-time security operations center capability.
Primary Objective: To identify the most critical information systems, develop visibility into cybersecurity posture of those systems, and ensure a whole-of-government approach to effectively manage risk.

Scope: All federal CFO and non-CFO act agencies. Over 820 HVAs self-identified.

Authorities: FISMA 2014 - OMB M-19-03 and BOD 18-02


Contact info: hvapmo@hq.dhs.gov
Next Steps and Ongoing Interagency Collaboration

**Comment adjudication:**
- **133 comments** from **10 organizations** on Draft SP 800-171, Rev 2
- **644 comments** from **46 organizations** on Draft SP 800-171B
  - All public comments received during comment period on Draft SP 800-171B are posted on NIST Protecting CUI Website

**Pending release of NIST SP 800-171B and NIST SP 800-53, Rev. 5, update** to the DHS HVA Overlay and development of additional resources

**How do NIST and DHS continue to promote and improve contractor security within our respective missions and scopes?**
QUESTIONS

NIST Protecting CUI website (with new FAQ):
https://csrc.nist.gov/Projects/protecting-controlled-unclassified-information

NIST Cybersecurity Publications: https://csrc.nist.gov

DHS High Value Asset Program links:
https://cyber.dhs.gov/bod/18-02
https://www.dhs.gov/publication/high-value-asset-control-overlay

HVA Program Management Office:
hvapmo@hq.dhs.gov

Alan McClelland: alan.mcclelland@hq.dhs.gov

NIST Risk Management Framework Team:
sec-cert@nist.gov

Victoria Yan Pillitteri: victoria.yan@nist.gov