Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations (NIST SP800-171 Revision 1)

Today’s Presenter:
Wade Kastorff
SRC, Commercial Cyber Security Services

February 21, 2017

Moderator:
Steve Warzala
swarzala@quanterion.com
NIST Special Publication 800-171 Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

An Evolutionary Process
We are here to discuss

- What is the government attempting to protect?
- Changes to NIST SP 800-171 Revision 1
- Discoveries and Experiences
- Implementing NIST SP 800-171 Revision 1
What is the government attempting to protect?

Controlled Unclassified Information
Controlled Unclassified Information (CUI) is unclassified information that requires additional protections.

CUI Registry Categories and Subcategories

- Agriculture
- Controlled Technical Information
- Critical Infrastructure Subcategories:
  - Ammonium Nitrate
  - Chemical-terrorism Vulnerability Information
  - Critical Energy Infrastructure Information
  - DoD Critical Infrastructure Security Information
  - Physical Security
  - Protected Critical Infrastructure Information
  - Water Assessments
- Emergency Management
- Export Control Subcategories:
  - Research

CUI Registry Category-Subcategory Markings

<table>
<thead>
<tr>
<th>Category - Subcategory</th>
<th>Marking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture</td>
<td>AG</td>
</tr>
<tr>
<td>Controlled Technical Information</td>
<td>CTI</td>
</tr>
<tr>
<td>Critical Infrastructure</td>
<td>CRIT</td>
</tr>
<tr>
<td>Critical Infrastructure-Ammonium Nitrate</td>
<td>CRITAN</td>
</tr>
<tr>
<td>Critical Infrastructure-Chemical-terrorism Vulnerability Information</td>
<td>CVI</td>
</tr>
<tr>
<td>Critical Infrastructure-Critical Energy Infrastructure Information</td>
<td>CEII</td>
</tr>
<tr>
<td>Critical Infrastructure-DoD Critical Infrastructure Security Information</td>
<td>DCRIT</td>
</tr>
</tbody>
</table>

These are examples of the 129 Registry Categories and Subcategories and 103 Registry Markings. Full list is available at: https://www.archives.gov/cui/registry

Contact your security officer, classification specialist, and contracting officer for contract specific guidance on CUI.
## Covered Defense Information

### Controlled Technical Information

- **Technical information** with military or space application
  - Subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
  - Information, if disseminated, for distribution statements B through F, using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents.
  - Does not include information that is lawfully publicly available without restrictions.

### Critical Information (OPSEC)

- **Critical Information** (operations security) is specific facts identified through the Operations Security process about:
  - Friendly intentions
  - Capabilities
  - Activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment

### Export Control Information

- **Export control Information** is unclassified information concerning certain:
  - Items
  - Commodities
  - Technology Software
  - Other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives
  - Includes dual use items; items identified in export administration regulations, international traffic in arms (ITAR) regulations, and munitions list; license applications; and sensitive nuclear technology information

### Additional Definitions

- **Contractor attributional/proprietary information:**
  - Information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

- **Contractor information system:**
  - An information system belonging to, or operated by or for, the Contractor.
Challenges with CUI

- Many government organizations provide differing CUI definitions...
- For specific contractual guidance consult with your contracting officer or security officer
- Be prepared for change
Changes to NIST 800-171 Revision 1
An indicator of things to come

NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-171

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce
Where did “Information” go?

Definition and Usage of the Term Information System

Unless otherwise specified by legislation, regulation, or governmentwide policy, the use of the term information system in this publication is replaced by the term system. This change reflects a more broad-based, holistic definition of information systems that includes, for example: general purpose information systems; industrial and process control systems; cyber-physical systems; and individual devices that are part of the Internet of Things. As computing platforms and technologies are increasingly deployed ubiquitously worldwide and systems and components are connected through wired and wireless networks, the susceptibility of Controlled Unclassified Information to loss or compromise grows—as does the potential for adverse consequences resulting from such occurrences.

<table>
<thead>
<tr>
<th>information system [44 U.S.C., Sec. 3502]</th>
<th>A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>See Information System.</td>
</tr>
</tbody>
</table>
Chapter three is the heart of the publication and specifies the requirements for compliance, and states in part:

“Nonfederal organizations should describe in a system security plan, how the specified security requirements are met or how organizations plan to meet the requirements.”

“When requested, the system security plan and any associated plans of action for any planned implementations or mitigations should be submitted to the responsible federal agency/contracting officer to demonstrate the nonfederal organization’s implementation or planned implementation of the security requirements.”

“Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether or not it is advisable to pursue an agreement or contract with the nonfederal organization.”
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.\textsuperscript{26}

Footnote 26: There is no prescribed format or specified level of detail for system security plans. However, organizations must ensure that the required information in 3.12.4 is appropriately conveyed in those plans.
3.1.19: Encrypt CUI on mobile devices and mobile computing platforms.\textsuperscript{21}

Footnote 21: Mobile devices and mobile computing platforms include, for example, smartphones, tablets, E-readers, and notebook computers.

3.5.10 Store and transmit only cryptographically-protected passwords.
3.13.12: Prohibit remote activation\textsuperscript{27} of collaborative computing devices and provide indication of devices in use to users present at the device.

Footnote 27: Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.
“Finally, NARA, in its capacity as the CUI Executive Agent, also plans to sponsor in 2017, a single Federal Acquisition Regulation (FAR) clause” …

Last paragraph, buried in the middle: “The CUI FAR clause will also address verification and compliance requirements for the security requirements in NIST Special Publication 800-171.”

Reference, NIST SP 800-171r1, Page v
Discoveries and Experiences

It has been an interesting year
Large contractors were quick to notify their sub-contractors of NIST SP 800-171 and FAR/DFAR responsibilities…

Cybersecurity/IT professionals collaborated with various other organizational offices, e.g.: Contracting, Legal, Finance, Compliance, Program Management, and Security

Companies identified a need for Cybersecurity professionals

Inconsistent guidance -- is consistent

Requirements prove to be more difficult to engineer and expensive to deploy

Funding must be planned in advance

Cybersecurity Training
Experiences

- Government initially unprepared to provide key indicators or guides for data types
- CUI data was not segregated from other forms of data
- Workstations with access to CUI in public spaces were left unattended with no screen lock
- Differing technical methods for protecting access to data
- In place auditing was insufficient to address requirements
- CUI data is everywhere – test equipment, mobile devices, laboratory equipment, test beds, anechoic chambers, thumb drives, email, back-ups, manufacturing equipment, and products with reused code being shipped
Implementing NIST SP 800-171

Where should the organization be on this journey?
Roadmap to Implementing NIST 800-171

- Establish your cyber security baseline
- Develop a formal project plan for an enterprise IA program
- Obtain buy-in from the Executive Leadership Teams and/or Board of Directors
- Implement the multi-phase IA program plan.
- Conduct various self-assessment activities during and at the end of identified milestones
- Validate your cyber security posture at each significant milestone
Implement multi-factor authentication
- Something you know (Password)
- Something you have (Token, Smartcard)
- Something you are (biometrics)

Develop, deploy, exercise Cyber Incident Response Plan/Program

Plan of Actions and Milestones (POA&M) and System Security Plan to demonstrate ‘171 adherence

Controlled Unclassified Information
- Who is responsible for identifying types of CUI data?
- Where is CUI data on the enterprise?
- Can we isolate CUI on the enterprise?
References and Links

- Controlled Unclassified Information: https://www.archives.gov/cui/
- NIST SP 800-171r1: https://doi.org/10.6028/NIST.SP.800-171r1
14685 Avion Parkway
Chantilly, VA 20151
Phone: 703.961.5500
www.srcinc.com

Wade Kastorff
571.299.8372
wkastorff@srcinc.com

Chris Prentiss
703.961.5534
cprentiss@srcinc.com