Safeguarding Controlled Unclassified Information and Cyber Incident Reporting

Kevin R. Gamache, Ph.D., ISP®
Facility Security Officer

Why Are We Seeing These Rules?

“Stolen data provides potential adversaries extraordinary insight into the United States' defense and industrial capabilities and allows them to save time and expense in developing similar capabilities. Protection of this data is a high priority for the Department and is critical to preserving the intellectual property and competitive capabilities of our national industrial base and the technological superiority of our fielded military systems.”

Secretary of Defense Chuck Hagel – October 10, 2013 Memorandum

What is Controlled Unclassified Information?

- Any information that law, regulation, or government wide policy requires to have safeguarding or dissemination control

What is NIST 800-171?

- Information security standards and guidelines for Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- Is intended for use by federal agencies when agencies are providing CUI to nonfederal organizations (or when CUI is developed by those organizations for federal agencies)

What is NIST 800-171?

- The requirements apply only to components of nonfederal information systems that process, store, or transmit CUI, or provide security protection for such components.

Controlled Unclassified Information

President's Memorandum May 7, 2008

- A category designation for unclassified information that does not meet the standards for National Security Classification.
  - Pertinent to the national interests of the U.S. and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

Task Force Findings

117 different SBU markings currently in use.

- Executive branch suffers immensely from interagency inconsistent policies for sensitive information
- Frequent uncertainty as to what policies apply to sensitive info
- Inconsistent application of similar policies across agencies
- Absence of effective training, oversight and accountability. Tendency to over protect information, and diminish government transparency.

NIST 800-171

What are the basic requirements?

Safeguard

Applies for any CDI residing on or transiting through system

Report

Must be done within 72 hours of "discovery of any cyber incident" that affects CDI

If Contractor may receive DoD CDI (marked in accordance with DoD Inst. 5230.24)

Contractor implements controls specified in NIST Special Pub. 800-171

Contractor explains to CO how controls not applicable or how alternate controls will work

Incident involving exfiltration, manipulation, loss or compromise, or unauthorized access of CDI

Contractor reports incident to DOD within 72 hours

Contractor investigates incident and preserves images for 90 days pending follow up by Govt.

Applicability

- All DoD solicitations and contracts
- Safeguarding requirements apply to Controlled Unclassified Information residing in, or transiting through, covered contractor information systems
- Compliance is required when contract is awarded. Full implementation is required NLT December 31, 2017

Covered Defense Information

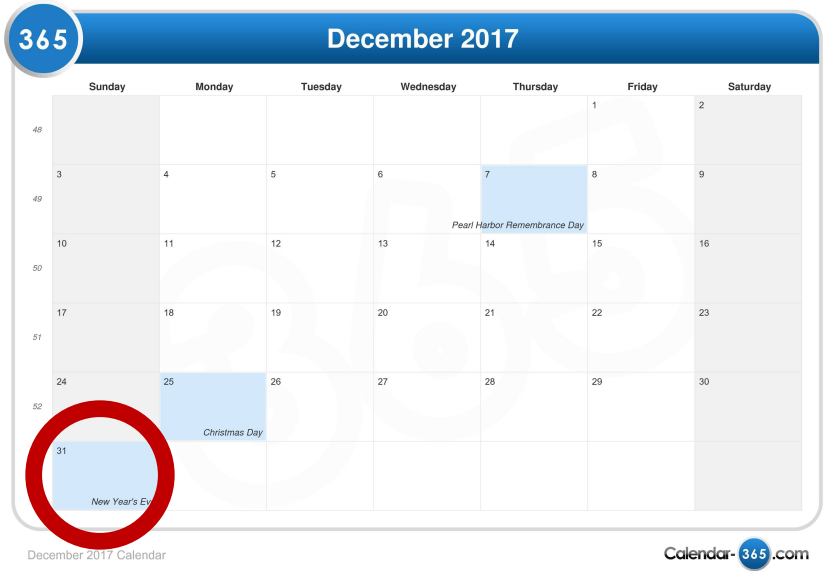
- Information that is
  - Provided to the contractor by or on behalf of DoD in connection with the performance of the contract;
  - Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract and that also falls into any of the following categories:

Covered Defense Information

- Controlled technical information,
- Critical information
- Export control information
- Any additional information marked or otherwise identified in the contract that is subject to controls imposed by law, regulation, or government-wide policy.

Adequate Security

- Contractor must implement protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information



Information System Security Requirements

- Access control
- Awareness and training
- Audit and accountability
- Configuration management
- Identification and authentication
- Contingency planning
- Incident response
- Maintenance
- Media protection
- Physical and environmental protection
- Program management
- Risk assessment
- Systems/ communications protection
- Systems / information integrity

Cyber Incidents

An unauthorized disclosure or release of Controlled Defense Information

Reporting requirements have twin purposes. One is to inform the DoD customer of potential injury from loss of its controlled data. The other is to inform DoD of how the attack occurred so that it can improve cyber defenses and better address threats.

Cyber Incident Reporting Requirements

(c) *Cyber incident reporting requirement.*

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.

- Cyber incidents must be reported within 72 hours
- Requires a DoD-approved medium assurance certificate

Issues to Consider

- Providing “adequate security” is a dynamic, not static obligation.
- The rule could impact organizational structure and operations.
- Some organizations may segregate compliant CDI from non-compliant systems.

Issues to Consider

- Cyber assurance may limit access via mobile and personal devices and affect telework.
- The rule will affect dealings with subcontractors.
- Care must be taken to flow down requirements and assure compliance.
- Subcontractors must confirm and adhere to reporting requirements.

Protection of Controlled Unclassified Information

- **Controlled Unclassified Information (CUI) is information that has not been given a security classification but which is withheld from public disclosure such as:**
  - Private Information
  - Export Controlled Information
  - Sensitive But Unclassified (SBU)
  - For Official Use Only (FOUO)
  - Proprietary Proposal Information
  - Company Proprietary / Private Information
  - Competition Sensitive
  - Personally Identifiable Information (PII)
- **The loss, theft, or corruption of this information would likely have a serious or detrimental impact on the execution of a contractor's programs and/or its personnel**

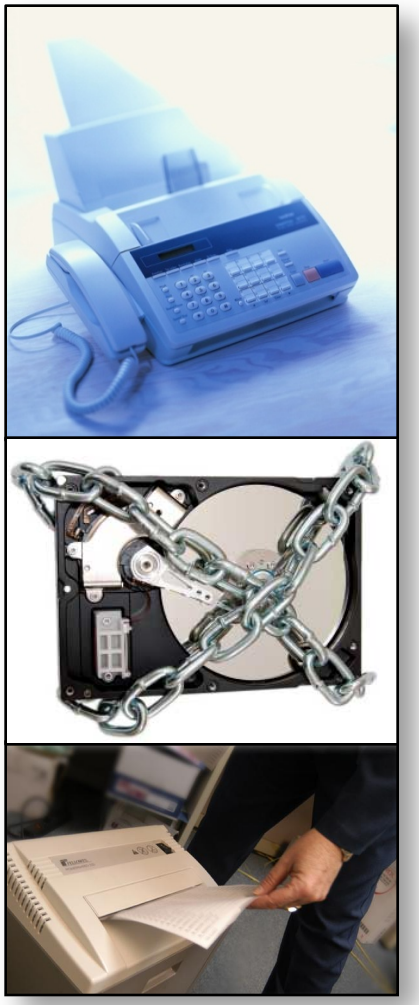
Protection of Controlled Unclassified Information

- **Protection measures may vary depending on the environment in which the information is stored or handled**
- **Environments are defined as:**
  - Protected Environment
    - Area where contractor controls access (proximity readers, security officers, etc.) to help ensure that only authorized employees, resident subcontractors, and visitors are permitted entry
  - Unprotected Environment
    - Area where contractor does not control access to building or work area (e.g., applicable remote sites and unprotected areas during business travel such as airplane cabins, coffee shops, etc.)

Protection of Controlled Unclassified Information

- **While in unprotected environments individuals must**
  - Be cognizant of their surroundings while viewing and processing this information
  - Take precautions to avoid unauthorized disclosure or loss
    - Use laptop privacy screens and unclassified coversheets
    - Encrypt all systems, media, and devices leaving contractor facilities
    - Any loss should be reported to the Security Department
- **While in protected environments individuals must**
  - Attach unclassified coversheet to material
  - Store in unlocked file, desk, office, or briefcase, or obscure from unauthorized viewing as a minimum

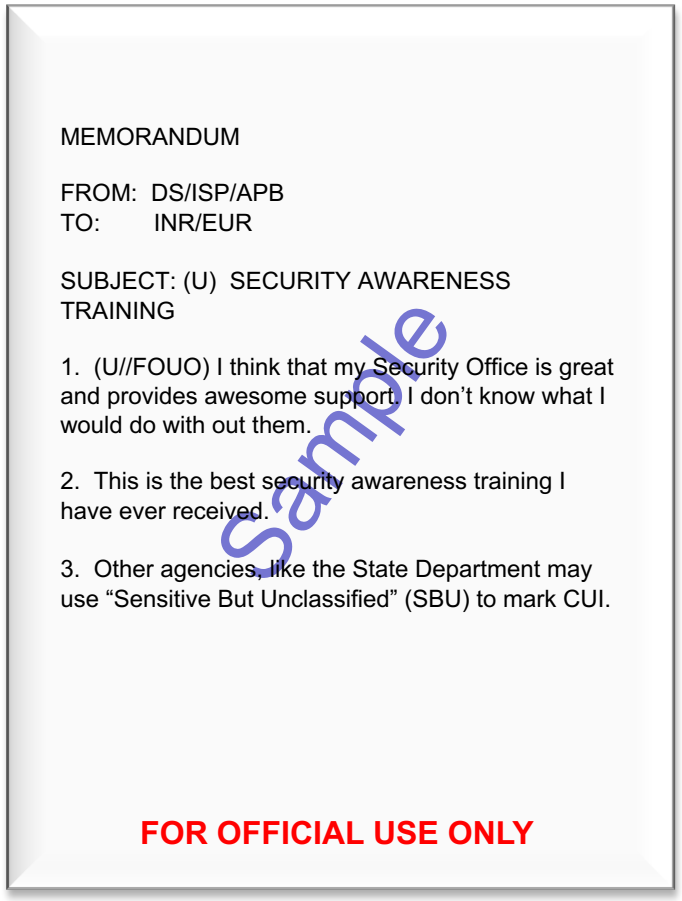
Protection of Controlled Unclassified Information



- **When sending or receiving sensitive unclassified information individuals must**
  - Implement need-to-know criterion
  - Employ available methods of safeguarding data while in transit (i.e., digital signatures, encryption methods, and classified fax machines, first class mail, password protected email attachments, etc.)
- **When no longer required, materials containing sensitive unclassified information will be promptly destroyed**
  - Cross-cut shred or dispose in shredder bins
  - Sanitize IT systems
- **Information owner may have additional protection requirements that will be addressed on a case-by-case basis**

Protection of Controlled Unclassified Information

- **Controlled unclassified documents should be marked accordingly:**
  - Bottom labeled appropriately (i.e., "For Official Use Only")
  - Outside of the front cover
  - On each page containing controlled unclassified information
  - Other material (i.e., slides, photos) will be marked to make recipients aware of the sensitivity
- **Controlled unclassified material being transmitted outside the DoD or its contractors facilities requires a statement explaining the marking**
  - "This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA. Exemptions… (list FOIA exemption being used)… apply"



Protection of Controlled Unclassified Information

- **Physical Protection measures:**
  - Maintain a need-to-know principle
  - Utilize Unclassified protection coversheets and notice labels (if available/used)
    - When at rest, hand carrying, sending via interoffice mail, or faxing (external mail, only use coversheets)
  - Use copiers or printers without hard drives, if available
    - If unavailable, device hard drives must be destroyed or sanitized when no longer used by contractor
  - Lock in a cabinet, desk, or office, or properly destroy if no longer required

Protection of Controlled Unclassified Information

- **Physical Protection measures:**
  - Use proper disposal and destruction methods
    - Destruction Bags (If used, maintain positive control at all times)
    - Shredders
  - Use data encryption for internal and external transmittal
  - Use password protected screensavers (Always lock your system when leaving your work area)
  - When possible, whole disk encryption should be implemented on systems containing this information