Sandia National Laboratories

Exceptional service in the national interest

Information Security- Subgroup

May 1-4, 2023

EFCOG S&S Working Group- Hosted by PNNL

SAND2023-03273C

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Overview

Security Briefing - Presentation & discussion must be unclassified.

Agenda:

Tuesday	Wednesday
Discuss CMPC assessment approach at your sites	Discuss marking classified in the digital environment
Discuss destruction of classified storage media	Discuss update to DOE O 471.6, Chg. 4 Information Security
Roundtable	Roundtable

Goal: Brief S&S group on Thursday about discussion and possible actions from this working group.

CMPC Assessments/Audits

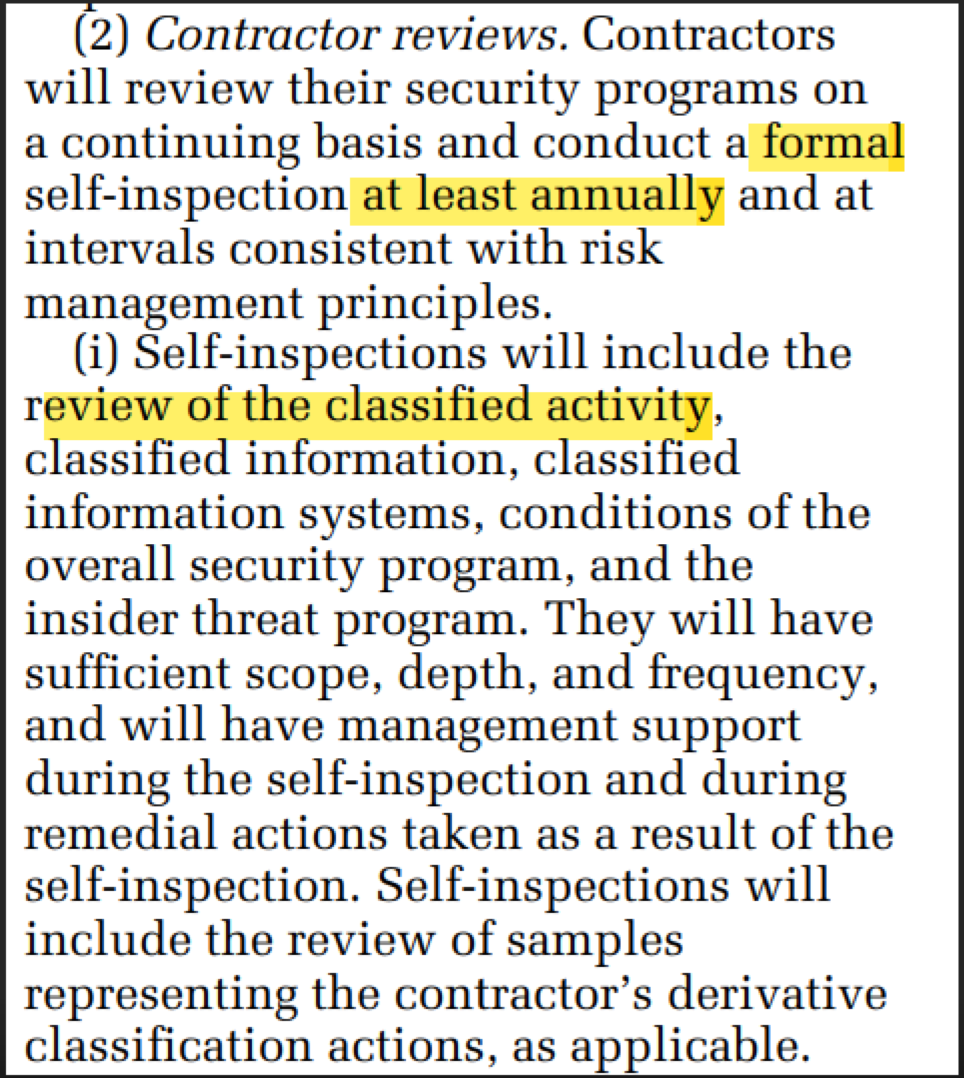
Agenda:

- Review related federal policies on assessments
- Discuss assessment approach used at your site (e.g., integration with other S&S Depts/federal oversight, management of non-compliances, lessons learned)

Goal: Identify any tools, checklists, processes that can be shared

Federal Policies

32 CFR Part 117, *National Industrial Security Program Operating Manual (NISPOM)*

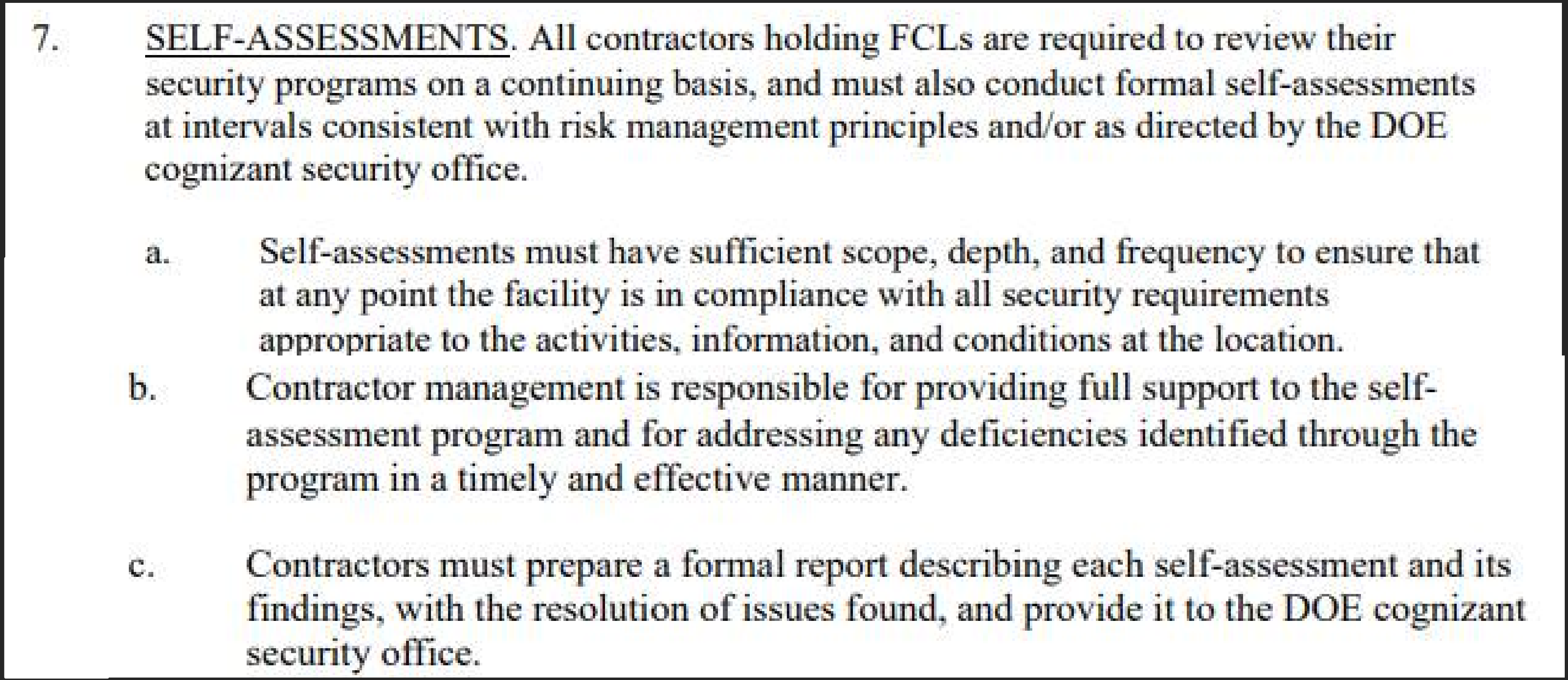


(2) *Contractor reviews.* Contractors will review their security programs on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles.

(i) Self-inspections will include the review of the classified activity, classified information, classified information systems, conditions of the overall security program, and the insider threat program. They will have sufficient scope, depth, and frequency, and will have management support during the self-inspection and during remedial actions taken as a result of the self-inspection. Self-inspections will include the review of samples representing the contractor's derivative classification actions, as applicable.

Federal Policies

DOE O 470.4B, Safeguards and Security Program



7. SELF-ASSESSMENTS. All contractors holding FCLs are required to review their security programs on a continuing basis, and must also conduct formal self-assessments at intervals consistent with risk management principles and/or as directed by the DOE cognizant security office.

   a. Self-assessments must have sufficient scope, depth, and frequency to ensure that at any point the facility is in compliance with all security requirements appropriate to the activities, information, and conditions at the location.

   b. Contractor management is responsible for providing full support to the self-assessment program and for addressing any deficiencies identified through the program in a timely and effective manner.

   c. Contractors must prepare a formal report describing each self-assessment and its findings, with the resolution of issues found, and provide it to the DOE cognizant security office.

CMPC Assessment Practices

Discussion:

1. What type of CMPC self-assessment activities are performed at your site? Are they compliance-based or are alternative assessment approaches used?

2. Who conducts CMPC assessments at your site? Your team, or a different entity (e.g., local federal field office)? Do you partner with other S&S Depts?

3. How do you manage and resolve non-compliances?

Goal: Any tools, checklists, processes you are willing to share?

DISCUSSION

Destruction of Electronic Storage Media

Challenges:

- Traditional electronic storage media (ESM) is quickly evolving and becoming more difficult to identify.
- Computers are not the only pieces of equipment with ESM.
- Volatile vs. Non-volatile Memory.

Electronic Storage Media Destruction

Discussion Starters:

1. What methods do you use to destroy classified ESM?

2. How do you ensure computers or equipment are free from nonvolatile ESM? Do you partner with your Cyber Security / IT POCs?

3. Will CUI impact your existing destruction approach for classified?

Goal: Identify approaches that help ensure classified ESM is always appropriately destroyed (per NSA's EPL).

DISCUSSION

Marking Classified in Digital Environment

Agenda:

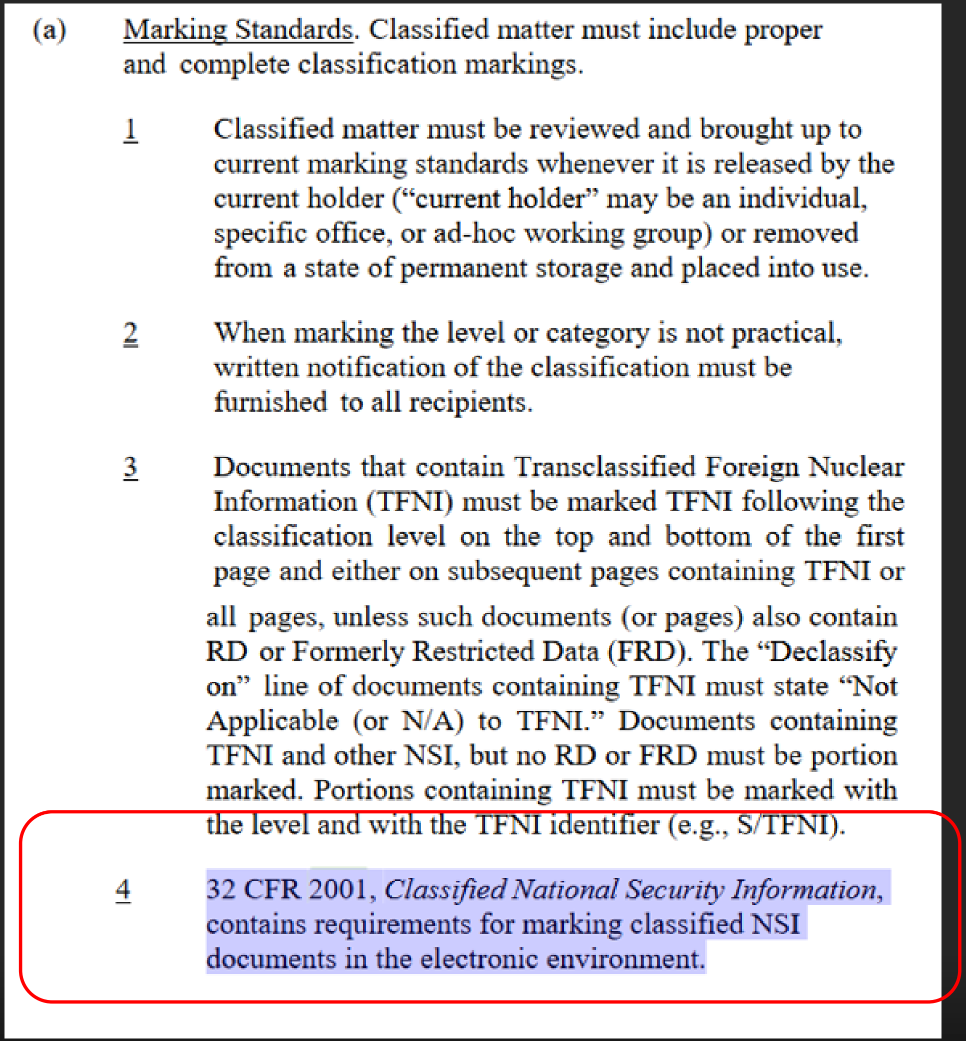
- Review related federal policies on classified marking

- Discuss marking challenges

Goals:

- Identify existing resources.
- Share local marking resources with each other?
- Provide recommendations to DOE HQ Policy POCs for consideration to grow the CMPC Marking Resource

Federal Policies



(a) Marking Standards. Classified matter must include proper and complete classification markings.

1 Classified matter must be reviewed and brought up to current marking standards whenever it is released by the current holder ("current holder" may be an individual, specific office, or ad-hoc working group) or removed from a state of permanent storage and placed into use.

2 When marking the level or category is not practical, written notification of the classification must be furnished to all recipients.

3 Documents that contain Transclassified Foreign Nuclear Information (TFNI) must be marked TFNI following the classification level on the top and bottom of the first page and either on subsequent pages containing TFNI or all pages, unless such documents (or pages) also contain RD or Formerly Restricted Data (FRD). The "Declassify on" line of documents containing TFNI must state "Not Applicable (or N/A) to TFNI." Documents containing TFNI and other NSI, but no RD or FRD must be portion marked. Portions containing TFNI must be marked with the level and with the TFNI identifier (e.g., S/TFNI).

4 32 CFR 2001, *Classified National Security Information*, contains requirements for marking classified NSI documents in the electronic environment.

DOE O 471.6, Chg. 3, Information Security

Multiple federal POCs have conveyed the identified section is applicable to all classified (e.g., RD/FRD) and not just NSI

Federal Policies

“Marking classified information with appropriate classification markings serves to warn and inform holders of information of the degree of protection required.”

“Since the primary purpose of the markings is to alert the holder that the information requires special protection, it’s essential that all classified material be marked to the fullest extent possible to ensure necessary safeguarding.”

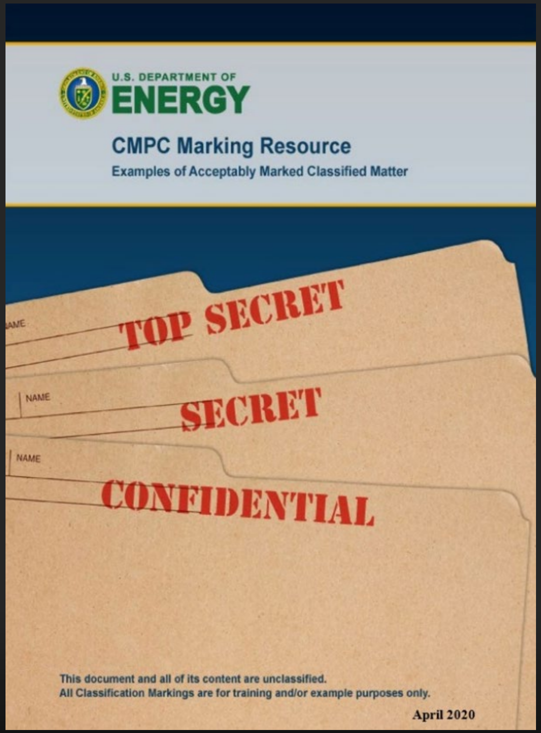
-32 CFR Part 117, *National Industrial Security Program Operating Manual (NISPOM)*

Federal Policies

Markings and designations serve two primary purposes:

- *Alert holders to the presence of classified information*
- *Warn holders of special access or safeguarding requirements*

-Dept of Energy CMPC Marking Resource



U.S. DEPARTMENT OF
ENERGY

CMPC Marking Resource

Examples of Acceptably Marked Classified Matter

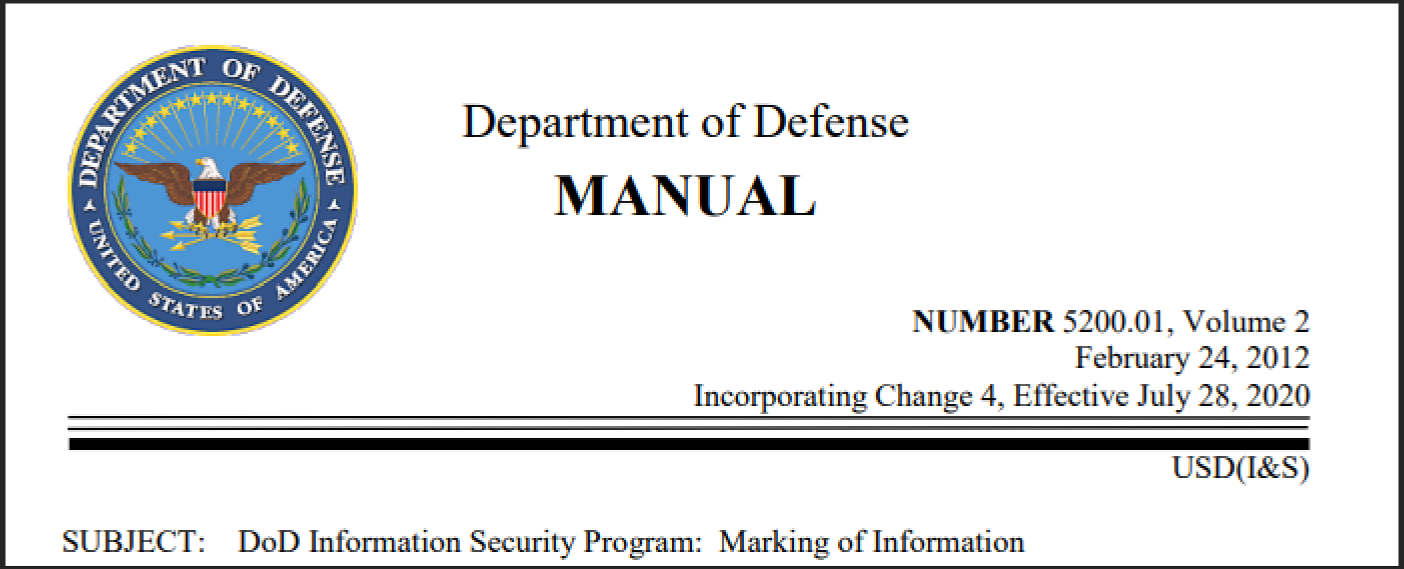
This document and all of its content are unclassified.
All Classification Markings are for training and/or example purposes only.

April 2020

"If markings cannot be affixed to specific classified information or materials, the originator shall provide holders or recipients with written instructions for protecting the information."

-32 CFR 2001

Federal Policies



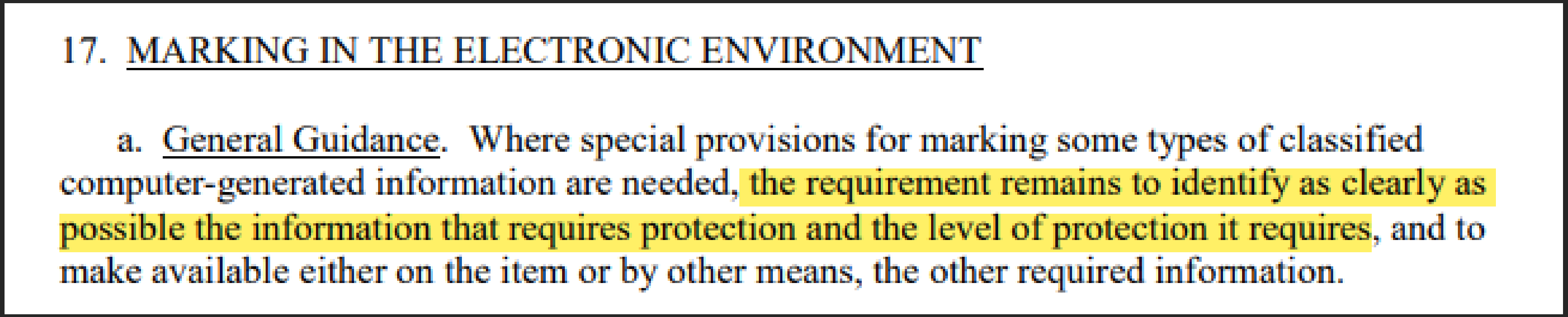
Department of Defense

MANUAL

NUMBER 5200.01, Volume 2
February 24, 2012
Incorporating Change 4, Effective July 28, 2020

USD(I&S)

SUBJECT: DoD Information Security Program: Marking of Information



17. MARKING IN THE ELECTRONIC ENVIRONMENT

a. General Guidance. Where special provisions for marking some types of classified computer-generated information are needed, the requirement remains to identify as clearly as possible the information that requires protection and the level of protection it requires, and to make available either on the item or by other means, the other required information.

Marking Classified in Digital Environment

Challenges:

- How to mark complex/non-traditional files?

- Compliance with the 180 day draft/working paper requirement in digital environment.

- Consistency of markings across the DOE/NNSA and contractor sites, especially on digital collaborative locations.

Marking Classified in Digital Environment

Discussion:

1. Does your site's policy covey expectation to mark digital classified items? Do you provide guidance for non-traditional files?
2. Has your site deployed any classified marking tools, besides for email? Examples- for MS products, pdf files, IM tools?
3. How do you assess markings in the electronic environment?

Goals

1. Identify existing resources.
2. Share local marking resources with each other? Any automated marking tools that can be recommended complex-wide?
3. Provide updated examples to DOE HQ Policy POCs for consideration to grow the CMPC Marking Resource

Update to DOE O 471.6, Chg. 4

Summary:

- Notice from RevCom on update to DOE O 471.6, Chg. 4 came in early-April 2023 with request for comments by mid-April.
- Comment resolution slated in RevCom to conclude May 19, 2023.
- Most changes made to CMPC portion were administrative (e.g., links, references) with exception of storage and OPSEC sections.

DOE O 471.6, Chg. 4 - RevCom

Discussion:

1. Are you included in updates to directives via RevCom?

https://www.directives.doe.gov/revcom

U.S. DEPARTMENT OF ENERGY

Directives Program,
Office of Management (MA-1.2)

2. Did your site provide comments/edits on any changes and/or existing requirements?

DISCUSSION

Sandia National Laboratories

Exceptional service in the national interest

Information Security
CMPC and OPSEC Sub-groups Debrief

Jeremy Pacheco- Sandia
Alma Farr- Pantex

May 4, 2023

EFCOG S&S Working Group- Hosted by PNNL

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Information Security Sub-Group: CMPC & OPSEC

CMPC Sessions:

1. CMPC Assessment Approach

   Actions:

   - Share tools used (e.g., checklists, forms, processes)
   - Share lessons learned

2. Destruction of Classified Electronic Storage Media

   Actions:

   - Potentially share ODFSA process/documentation for permanent burial
   - Share examples of marked media

Information Security Sub-Group: CMPC & OPSEC

CMPC Sessions (cont'd):

3. Marking Classified in Digital Environment

   Actions:

   - Collect recommendations to send to DOE HQ for consideration to add to the CMPC Marking Resource
   - Further discuss complex-wide tools to aid in marking.

4. Current update to DOE O 471.6, Chg. 4

   Actions:

   - Continue to share RevCom requests with each other
   - Consider participating on IPT team when re-write comes due

Information Security Sub-Group: CMPC & OPSEC

OPSEC Sessions:

1. Missed NA-70 SME's presence

2. National Training Center inputs and assistance

3. OPSEC Strategic Plan – Five years out
   - Standardizing templates
   - Lines of Inquiry
   - OPSEC Exchange Program – visit each other's sites to perform assessment

Information Security Sub-Group: CMPC & OPSEC