

NNSA POLICY

NAP 470.1

Approved: 08-18-23
Recertification Due: 08-18-26

ENHANCED COMPENSATORY CONTROL MEASURES



NATIONAL NUCLEAR SECURITY ADMINISTRATION **Office of Defense Nuclear Security**

CONTROLLED DOCUMENT
AVAILABLE ONLINE AT:
<http://directives.nnsa.doe.gov>

OFFICE OF PRIMARY INTEREST (OPI):
Office of Defense Nuclear Security

printed copies are uncontrolled

THIS PAGE INTENTIONALLY LEFT BLANK

ENHANCED COMPENSATORY CONTROL MEASURES

1. PURPOSE. To implement Enhanced Compensatory Control Measures (ECCM) to improve the protection of sensitive information, operations, or activities through a formalized application of supplemental security measures based on identified risk. ECCMs are used for the authorization, management, integration, and oversight of National Nuclear Security Administration (NNSA) programs with activities where standard security measures are determined to be insufficient to enforce need-to-know restrictions and where Special Access Program (SAP) or Sensitive Compartmented Information (SCI) controls are not warranted or approved.
2. AUTHORITY. NNSA's directive program is established under 50 United States Code (U.S.C.) 2402(d), *Administrator for Nuclear Security*. This law gives the Administrator authority to establish NNSA-specific policies, unless disapproved by the Secretary.
3. CANCELLATION. None.
4. APPLICABILITY.
 - a. Federal. Applies to all federal NNSA elements.
 - b. Contractors. The Contractor Requirements Document (CRD), included as Attachment 1, sets forth requirements of this directive that apply to contractors. The CRD also includes Attachments 2-5. All must be included in Management and Operating contracts and provided to all NNSA prime contractors, including contracts performing classified work which require ECCM security measures.
 - c. Equivalencies/Exemptions.
 - (1) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 U.S.C. sections 2406 and 2511, and to ensure consistency throughout the joint Navy/ Department of Energy (DOE) Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.
 - (2) Equivalency and exemption requests are processed through and approved by the applicable NNSA Program Office responsible for the activity requiring ECCM.
5. SUMMARY OF CHANGES. None.
6. BACKGROUND. This directive establishes requirements not contained in DOE policy. This NNSA Policy (NAP) is intended to bridge the gap between existing policies for the protection of sensitive information, operations, or activities and where SAP or SCI controls are not warranted or approved. ECCM are a series of measures to deter and

detect activities like the subversion of critical program information or materials in an operational environment. This directive requires the programmatic establishment and implementation of additional security controls.

7. REQUIREMENTS.

a. ECCMs must:

- (1) Be approved by the appropriate head of an NNSA Program or Support Office who acts as the ECCM Sponsor. This approval is based on identifying when existing security measures are insufficient to protect sensitive activity.
- (2) Maintain an updated Access Control List (ACL) of authorized personnel.
- (3) Register administrative information into a centralized repository, including ECCM name, nickname, sponsor, control officer, contact information, date active, date deactivated, etc.
- (4) Not be used to deny information or access for authorized purposes.
- (5) Operate in accordance with an approved ECCM Plan. At a minimum, the plan must include:
 - (a) Definition of the specific information, operations, or activities that require ECCM protection.
 - (b) Identification of the ECCM Sponsor and supporting organizational structure.
 - (c) Identification of competing policies, requirements, or practices that would impair or inhibit the implementation of the ECCM.
 - (d) Identification and documentation of appropriate mitigations or exemptions, as necessary.
 - (e) Identification and quantification of adverse impacts (e.g., risk, budget, schedule, quality) that are likely to occur as a result of implementing ECCM.
 - (f) Physical locations where ECCM work will be performed.
 - (g) The unclassified nickname for the specific ECCM.

Note: The use of classified nicknames, codewords, or program numbers is not authorized.

- (h) Involvement of Other Government Agencies (OGA) and identification of a memorandum of understanding/agreement (MOU/MOA) where necessary.
- (i) Involvement of foreign nationals and the basis by which ECCM information exchange(s) will occur.
- (j) Identify reporting requirements and channels for conveying ECCM-related information.
- (k) Estimated duration of the ECCM.
- (l) Identification of restrictions and limitations on individuals involved in the ECCM and how those restrictions and limitations will be enforced. This information must be communicated to the individuals prior to being briefed into the ECCM.
- (m) Define procedure for reporting and response to inadvertent disclosure of ECCM information while incorporating other mandatory reporting requirements (e.g., Incidents of Security Concern, Occurrence Reporting and Processing System, Computerized Accident/Incident Reporting Systems)
- (n) Identify risk and control measures for external and internal threats or vulnerabilities. The plan should include consideration of the following:
 - 1 Physical and cyber security controls that address adversarial actions.
 - 2 Guidance on addressing adversarial subversion lifecycle (targeting, access, weaponization, deployment, command, and control).
 - 3 Evaluation of adversarial capabilities (tools, training, and knowledge) and threat forecasting.
 - 4 Leverage existing resources responsible for threat and vulnerability identification (e.g., Counterintelligence, Nuclear Enterprise Assurance, Safeguards and Security).
- (6) Identify responsible oversight authorities (e.g., audits, federal site responsibilities). Ensure existing programmatic requirements for oversight of activities contained within the ECCM are met.
- (7) Provide an ECCM-specific briefing to participants including requirements, responsibilities, restrictions, and reporting.

- (a) Briefings should occur upon entry into the ECCM and at regular intervals.
 - (b) Be tailored to include the specific information, operations, and activities subject to the ECCM in which the individual is involved, including any control measures applied and necessary classification guidance.
 - (c) Include an ECCM-specific briefing acknowledgement (Attachment 5), signed by the individual and ECCM Control Officer or Coordinator.
 - (d) Provisional ECCMs may be authorized on an emergency basis following notification to the cognizant NNSA Program or Support Office.
- b. Within 6 months of approval of this policy, the appropriate Head of NNSA Element who acts as the ECCM Sponsor must identify and formally approve all existing ECCM-like programs and issue program plans. Within 12 months of issuance of this policy, approved ECCMs must become compliant with the approved plans or submit an implementation plan to become compliant through the Field Office Manager or delegate to the appropriate Head of NNSA Element who acts as the ECCM Sponsor.

8. RESPONSIBILITIES.

- a. Associate Administrator and Chief for Defense Nuclear Security (NA-70).
 - (1) Develops and coordinates NNSA ECCM policy with stakeholders.
 - (2) Coordinates and deconflicts unclassified nickname designation with the Department of Defense and the ECCM Coordinator.
 - (3) Establishes and maintains a centralized repository where required ECCM administrative information is documented.
- b. ECCM Sponsor.
 - (1) Head of NNSA Element (e.g., NA-10, NA-20, NA-80) acts as the ECCM Sponsor who authorizes the activation, modification, or deactivation of ECCMs within their area of responsibility.
 - (2) Ensures that sufficient resources are planned, budgeted, and allocated in support of the ECCM.
 - (3) Appoints in writing the ECCM Control Officer(s) to manage the ECCMs established under their cognizance.

- (4) Ensures the ECCM complies with the requirements in this policy.

c. ECCM Control Officer.

- (1) Recommends the ECCM for approval, establishment, modification, or deactivation within their area of responsibility.
- (2) Identifies alternate ECCM Control Officers, as necessary.
- (3) Approves access into the ECCM and maintains the Access Control List (ACL) for active and inactive participants.
- (4) Identifies ECCM Coordinator(s) and defines their authority to approve access.
- (5) Coordinates annual reporting on the status of the ECCM and updates the centralized repository upon deactivation of the ECCM.
- (6) Approves provisional ECCMs.

d. ECCM Coordinator.

- (1) Implements the ECCM in accordance with the ECCM Plan.
- (2) Notifies the ECCM Control Officer of changes to the Access Control List.
- (3) Administers the day-to-day activities fulfilling ECCM requirements.
- (4) Reviews and provides recommendations for updates to the ECCM Plan.
- (5) Administers and executes briefing acknowledgments as provided by the ECCM Plan.
- (6) Reviews and provides recommendations for resolving security-related issues, security violations, or security incidents involving ECCM-related matters.

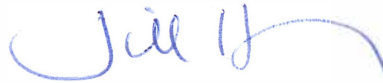
e. Field Office Manager or Delegate.

- (1) Reviews and concurs on project and program plans requiring ECCM protection.
- (2) Provides support and security oversight of the ECCM, as necessary.

f. Contracting Officers. Incorporate the CRD of this NAP into contracts within 6 months of the effective date of this NNSA directive or provide an implementation plan and schedule if this cannot be executed in the allotted time.

- g. Officially Designated Federal Security Authority (ODFSA) for NNSA Cyber Security. Provides support and cyber oversight of the ECCM as necessary.
- 9. DEFINITIONS. See Attachment 2.
- 10. ACRONYMS/ABBREVIATIONS. see Attachment 3.
- 11. REFERENCES. See Attachment 4.
- 12. CONTACT. Questions concerning this NAP should be addressed to the Office of Defense Nuclear Security (NA-70) at (202) 586-8900.

BY ORDER OF THE ADMINISTRATOR:



Jill Hruby
Administrator

Attachments:

- 1. Contractor Requirements Document (CRD)
- 2. Acronyms/Abbreviations
- 3. Definitions
- 4. References
- 5. Sample Briefing Acknowledgment Form

ATTACHMENT 1: CONTRACTOR REQUIREMENT DOCUMENT
NAP-470.1, *ENHANCED COMPENSATORY CONTROL MEASURES*

1. INTRODUCTION.

This Contractor Requirements Document (CRD) establishes the enterprise Enhanced Compensatory Control Measures (ECCM) requirements for National Nuclear Security Administration (NNSA) contractors supporting programs with activities where standard security measures are determined to be insufficient to enforce need-to-know requirements and where Special Access Program (SAP) or Sensitive Compartmented Information (SCI) controls are not warranted or approved.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD and for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In addition to the requirements of this CRD, contractors are subject to the information set forth in Attachments 1-5 of this directive.

Contractors may not establish an ECCM unless authorized by the ECCM Sponsor.

2. REQUIREMENTS. Contractors supporting ECCMs must:

- a. Operate in accordance with the approved ECCM Plan.
- b. Support approved ECCMs by providing necessary resources and staff as identified in the plan.
 - (1) M&O contractors may serve as an ECCM Coordinator and must fulfill obligations identified in accordance with the CRD Responsibilities section of this policy and the specific ECCM Plan.
 - (2) Contractors should be prepared to provide applicable resources (e.g., budgetary) documentation necessary to fulfill ECCM requirements.
- c. Assist in the development of ECCM Plans that, at a minimum, include:
 - (1) Definition of the specific information, operations, or activities that require ECCM protection.
 - (2) Identification of the ECCM Sponsor and supporting organizational structure.
 - (3) Identification of competing policies, requirements, or practices that would impair or inhibit the implementation of the ECCM.
 - (4) Identification and documentation of appropriate mitigations or exemptions, as necessary.

- (5) Identification and quantification of adverse impacts (e.g., risk, budget, schedule, quality) that are likely to occur because of implementing ECCM.
- (6) Physical locations where ECCM work will be performed.
- (7) The unclassified nickname for the specific ECCM.

Note: The use of classified nicknames, codewords, or program numbers is not authorized.
- (8) Involvement of Other Government Agencies (OGA) and identification of a memorandum of understanding/agreement (MOU/MOA) where necessary.
- (9) Involvement of foreign nationals and the basis by which ECCM information exchange(s) will occur.
- (10) Identify reporting requirements and channels for conveying ECCM-related information.
- (11) Estimated duration of the ECCM.
- (12) Identification of restrictions and limitations on individuals involved in the ECCM and how those restrictions and limitations will be enforced. This information must be communicated to the individuals prior to being briefed into the ECCM.
- (13) Define procedure for reporting and response to inadvertent disclosure of ECCM information while incorporating other mandatory reporting requirements (e.g., Incidents of Security Concern, Occurrence Reporting and Processing System, Computerized Accident/Incident Reporting Systems)
- (14) Identify risk and control measures for external and internal threats or vulnerabilities. The plan should include consideration of the following:
 - (a) Physical and cyber security controls that address adversarial actions.
 - (b) Guidance on addressing adversarial subversion lifecycle (targeting, access, weaponization, deployment, command, and control).
 - (c) Evaluation of adversarial capabilities (tools, training, and knowledge) and threat forecasting.
 - (d) Leverage existing resources responsible for threat and vulnerability identification (e.g., Counterintelligence, Nuclear Enterprise Assurance, Safeguards and Security).

- (15) Identify responsible oversight authorities (e.g., audits, federal site responsibilities). Ensure existing programmatic requirements for oversight of activities contained within the ECCM are met.
- d. Provide an ECCM-specific briefing to participants including requirements, responsibilities, restrictions, and reporting.
- e. Briefings should occur upon entry into the ECCM and at regular intervals and:
 - (1) Be tailored to include the specific information, operations, and activities subject to the ECCM in which the individual is involved, including any control measures applied and necessary classification guidance.
 - (2) Include an ECCM-specific briefing acknowledgement, signed by the individual and ECCM Control Officer or Coordinator.
- f. Within 6 months of approval of this policy, contractor personnel must identify all ECCM-like activities at their respective sites and provide notification of such through the Field Office Manager or delegate to the appropriate Head of NNSA Element who acts as the ECCM Sponsor. The appropriate Head of NNSA Element who acts as the ECCM Sponsor must formally approve all existing ECCM-like programs and issue program plans. Within 12 months of issuance of this policy, approved ECCMs must become compliant with the approved plans or submit an implementation plan to become compliant through the Field Office Manager or delegate to the appropriate Head of NNSA Element who acts as the ECCM Sponsor.

3. RESPONSIBILITIES.

- a. ECCM Coordinator.
 - (1) Implements the ECCM in accordance with the ECCM Plan.
 - (2) Notifies the ECCM Control Officer of changes to the Access Control List.
 - (3) Administers the day-to-day activities fulfilling ECCM requirements.
 - (4) Reviews and provides recommendations for updates to the ECCM Plan.
 - (5) Administers and executes briefing acknowledgments as provided by the ECCM Plan.
 - (6) Reviews and provides recommendations for resolving security-related issues, security violations, or security incidents involving ECCM-related matters.

ATTACHMENT 2: DEFINITIONS

Note: This attachment applies to contractor and federal organizations.

- a. Access Control List. List or roster used to control access to ECCM information. ACLs will also be used to establish discretionary access controls to limit access to ECCM material on electronic systems to only those personnel with need-to-know verified by the ECCM Control Officer. The ACL list consists of active and formerly active participants.
- b. Classified Information. Information that is classified by statute or Executive Order. Such information includes: (1) Restricted Data or Formally Restricted Data classified by the *Atomic Energy Act* or 10 Code of Federal Regulations part 1045; (2) Transclassified Foreign Nuclear Information classified by the *Atomic Energy Act*; and (3) National Security Information classified by Executive Order 13526 or prior Executive orders. (DOE O 475.2B).
- c. Enhanced Compensatory Control Measures. Protection of sensitive information, activities, and operations through formalized application of supplemental security measures based on identified risk. An ECCM is used to increase safeguards when normal or standard security measures are insufficient and where SAP or SCI controls are not required.
- d. Nickname. The unclassified, two-word ECCM designation derived from the Department of Defense nickname system, NICKA, and assigned by the NNSA Office of Defense Nuclear Security.

ATTACHMENT 3: ACRONYMS AND ABBREVIATIONS

Note: This attachment applies to NNSA contractor and federal organizations.

a.	ACL	Access Control List
b.	CRD	Contractor Requirements Document
c.	DOE	Department of Energy
d.	ECCM	Enhanced Compensatory Control Measures
e.	MOA	Memorandum of Agreement
f.	MOU	Memorandum of Understanding
g.	NAP	NNSA policy
h.	NEA	Nuclear Enterprise Assurance
i.	NNSA	National Nuclear Security Administration
j.	OGA	Other Government Agency
k.	SAP	Special Access Program
l.	SCI	Sensitive Compartmented Information
m.	U.S.C.	United States Code

ATTACHMENT 4: REFERENCES

Note: This attachment applies to NNSA contractor and federal organizations.

- a. *National Industrial Security Program Operating Manual* 32 C.F.R §117 (2014).
- b. Executive Order No. 13526, 75 Fed. Reg. 705 (2009).
- c. PPD- 35, *United States Nuclear Weapons Command and Control, Safety, and Security* (2015).
- d. NSPM-31, *United States Stockpile Stewardship and Nuclear Testing*.
- e. NSPM- 35, *National Technical Nuclear Forensics* (2021).
- f. NSPM-36, *Guidelines for United States Government Interagency Response to Terrorist Incidents in the United States and Overseas*.
- g. DOE O 452.7, Ch. 1, *Protection of Use Control Vulnerabilities and Designs* (2015).
- h. DOE O 452.8, *Control of Nuclear Weapon Data* (2011).
- i. DOE O 471.6, Ch.3, *Information Security* (2019).
- j. DoD-M 5200.01 V.3 *DoD Information Security Program Protection of Classified Information (ACCM section only)*.
- k. CJCSM 3213.02D, *Joint Staff Alternative Compensatory Control Measures (ACCM) Program Management Manual*.
- l. CJCSM 3150.29E, *Code Word, Nickname, and Exercise Term (NICKA) System*.
- m. NNSA NEA SD 452.4-1, *Nuclear Enterprise Assurance (NEA)* (2022).
- n. DOE O 452.2F, *Nuclear Explosive Safety* (2020).

ATTACHMENT 5: ENHANCED COMPENSATORY CONTROL MEASURES BRIEFING ACKNOWLEDGMENT FORM



CUI//OPSEC
(When completed)

ENHANCED COMPENSATORY CONTROL MEASURES BRIEFING ACKNOWLEDGMENT FORM



Name:	Agency:
Position/Title:	Organization:
Work Address:	Phone Number:

1. I acknowledge that I have received the Enhanced Compensatory Control Measure (ECCM) briefing on the specific requirements of the ECCM-(Nickname). I am aware that the unauthorized negligent handling or disclosure of ECCM information, could seriously affect the national security and that the transmission or revelation of sensitive information, operations, or activities to unauthorized persons could subject me to prosecution under applicable law of the United States, including but not limited to the Espionage Laws (U.S. Code Title 18, Section 793, 794, and 798 and U.S. Code Title 50, Section 783), and the Atomic Energy Act of 1954, as amended. I recognize that nothing in this Acknowledgment constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
2. I understand that this Acknowledgement does not supersede any other program specific (e.g., Sigma, Special Access Program, Human Reliability Program, Sensitive Compartmented Information, etc.) acknowledgements or the Standard Form 312, *Classified Information Nondisclosure Agreement* I may have signed.
3. I pledge that I will never publish, communicate, transmit, or reveal, by any means, ECCM information, operations, or activities to unauthorized persons or organizations. This also means I will submit any communication or work potentially involving the ECCM for review. I recognize and accept the fact that I have a personal responsibility to protect ECCM information that I have knowledge of and agree by the security requirements and regulations established under the Department of Energy (DOE), National Nuclear Security Administration (NNSA), and as outlined in the ECCM-(Nickname) Program Plan.
4. I understand that access to certain ECCM information does not entitle me access to other ECCMs. I understand that access is restricted to those who have a need-to-know for the specific information needed to perform their authorized duties. I am aware that this is my personal responsibility to confirm that any person to whom I release ECCM information is currently authorized to receive it and has a valid need-to-know.
5. In addition to existing security procedures established for the protection of classified and unclassified information, I have been briefed on additional security measures and program requirements under ECCM-(Nickname).

Controlled By: _____ (Organization)
CUI Category: _____ OPSEC
POC: _____ (Person, Phone)

CUI//OPSEC
(When completed)

CUI//OPSEC
(When completed)

6. I understand that my access to ECCM-(Nickname) may be terminated at any time and for any reason. I acknowledge that should my access be terminated, ECCM-related duties will be reassigned.
7. I will promptly notify the ECCM Coordinator if I am aware of an attempt to solicit ECCM information.
8. I will promptly notify the ECCM Coordinator in the event I encounter ECCM information in the public domain or other unauthorized locations.
9. I understand that once debriefed from ECCM-(Nickname), I will no longer be authorized to access ECCM information, operations, or activities. I understand that I must not inquire into, discuss, disclose, or speculate on any ECCM information, except as authorized by law, DOE/NNSA regulations, or in writing by the ECCM Sponsor.
10. Unless and until I am released in writing by an authorized representative of the U.S. Government, I understand all conditions and obligations imposed upon me by this Acknowledgment during the time I am granted access to ECCM-(Nickname), and at all times thereafter. I have read this Acknowledgement carefully and my questions, if any, have been answered.

Signature: _____ Date: _____

Print Name: _____

Signature of Briefer: _____ Date: _____

DEBRIEFING ACKNOWLEDGMENT

I affirm that I have returned all ECCM material(s) in my custody and that I will not share any knowledge of the ECCM-(Nickname) without proper approval from the NNSA. By my signature I acknowledge that, effective the date below, I am no longer authorized access to ECCM information, operations, or activities in accordance with the terms above. Despite termination of my access, I understand that I remain bound by my pledge to never publish, communicate, transmit, or reveal, by any means, ECCM information, operations or activities to unauthorized person or organizations.

Signature: _____ Date: _____

Print Name: _____

Signature of Debriefer: _____ Date: _____

CUI//OPSEC
(When completed)