

NAP 14.3-B

Approved: 05-02-08

**TRANSMISSION OF RESTRICTED DATA
OVER SECRET INTERNET PROTOCOL
ROUTER NETWORK (SIPRNet)**



**NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of the Chief Information Officer**

AVAILABLE ONLINE AT:
<http://hq.na.gov>

INITIATED BY:
Office of the Chief Information Officer

This page intentionally left blank.

Table of Contents

TRANSMISSION OF RESTRICTED DATA OVER SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNet)

1. PURPOSE	1
2. APPLICABILITY	1
3. CANCELLATIONS	2
4. RESPONSIBILITIES	2
5. REQUIREMENTS	2
6. CONTACT	4
APPENDIX A	
CONTRACTOR REQUIREMENTS DOCUMENT	A-1

This page intentionally left blank.

**TRANSMISSION OF RESTRICTED DATA OVER SECRET INTERNET PROTOCOL
ROUTER NETWORK (SIPRNET)**

1. **PURPOSE.** To establish requirements and responsibilities for operation of the Secret Internet Protocol Router Network (SIPRNet) Controlled Interface for the electronic transmission of Restricted Data (RD) between National Nuclear Security Administration (NNSA) information systems and SIPRNet.

2. **APPLICABILITY.** This NNSA Policy Letter (NAP) applies to all entities, Federal or contractor, that collect, create, process, transmit, store, or disseminate information on SIPRNet for the NNSA.
 - a. **NNSA Elements.** NNSA Headquarters Organizations, Service Center, Site Office, NNSA Management and Operating contractors, integrating contractors, and subcontractors are, hereafter, referred to as NNSA Elements

 - b. **Information System.** This NAP applies to any NNSA information system that collects, creates, processes, transmits, stores, or disseminates classified NNSA information. This NAP applies to any information system life cycle, including the development of new information systems, the incorporation of information systems into an infrastructure, the incorporation of information systems outside the infrastructure, the development of prototype information systems, the reconfiguration or upgrade of existing systems, and legacy systems. In this document, the term(s) "information system" or "system" are used to mean any information system or network that is used to collect, create, process, transmit, store, or disseminate data owned by, for, or on behalf of the NNSA or DOE.

 - c. **Contractors.** Except for the exclusions in paragraph 2.e, the Contractor Requirements Document (CRD), Appendix A, sets forth requirements of this policy that will apply to contractors whose contracts include the CRD.
 - (1) The CRD shall be included in NNSA site and/or facility management contracts that provide automated access to SIPRNet.

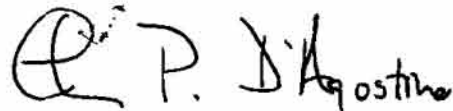
 - (2) Site and/or facility management contracts that have the CRD incorporated states, regardless of the performer of the work, site and facility management contractors are responsible for being in compliance with the requirements of the CRD.

 - (3) Affected contractors are responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the contractors' compliance with the requirements.

- d. Deviations. Deviations from the requirements prescribed in this NAP must be processed in accordance with the requirements in NAP 14.1-C, *NNSA Baseline Cyber Security Program*.
 - e. Exclusion. The Deputy Administrator for Naval Reactors shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (set forth in Public Law 106-65 of October 5, 1999 [50 U.S.C. 2406]) and to ensure consistency throughout the joint Navy and DOE Organization of the Naval Reactors Propulsion Program, implement and oversee all requirements and practices pertaining to this policy for activities under the Deputy Administrator's cognizance.
 - f. Implementation. A plan for the implementation of this NAP must be completed within 60 days after modification of the site's contract to include this NAP. A plan for the implementation of this NAP within an NNSA Federal organization must be completed within 60 days after issuance of this NAP. The implementation plan shall not exceed three years from the date of formal approval. Further, all information systems as defined in paragraph 2.b, must be protected in accordance with the requirements set forth in this NAP. The implementation plan must describe, at a minimum, the program activity to be modified and/or created; the starting date of revision and/or development; the estimated due date; and the responsible party for the stated activity.
3. CANCELLATIONS. This NNSA policy cancels NAP 14.13, *Transmission of Restricted Data (RD) and Formerly Restricted Data (FRD) over the Secret Internet Protocol Router Network (SIPRNet)*, dated April 5, 2006.
 4. RESPONSIBILITIES. Roles and responsibilities for all activities in the NNSA PCSP are described in NAP 14.1-C, *NNSA Baseline Cyber Security Program*.
 5. REQUIREMENTS.
 - a. RD, except for Sigmas 14, 15, 20, and Top Secret, may be transmitted via SIPRNet from a system that has been formally accredited to process, store, and transmit RD information.
 - b. The requirements and implementation of this NAP must be merged into the Information System Security Plan (ISSP) with those of DOE Manual 205.1-4, *National Security Systems Manual*, and be subjected to the NNSA Certification and Accreditation Process. The ISSP will include a description of the controlled interface technical and procedural agreements required for transmission, including clearance and briefings required for access to specific classification levels and categories of information, between the NNSA system and SIPRNet. The interconnection must be part of the Security Test and Evaluation Plan of the Certification and Accreditation process.

- c. This section describes the requirements for interconnecting the DOD SIPRNet and a DOE System and/or Network accredited for Confidential or Secret RD.
 - (1) The Access Authorization process, need-to-know, and access briefings must be validated; however, policy does not authorize the sender and/or DOD recipients to validate their own information.
 - (2) These authorizations must be re-validated at least monthly to ensure that they remain current.
 - (3) Processes must be established to ensure the following:
 - (a) A review of at least 20% of the e-mail, including attachments transmitted and/or received via this controlled interface to ensure that the e-mail does not contain RD that is unencrypted. Sigmas 14, 15, and 20 cannot be transmitted across SIPRNet.
 - (b) That all RD transmittals have been properly marked. Refer to the User Group Control Memo, dated January, 2006.
 - (c) Records of RD traffic must be maintained, in accordance with DOE records and the National Archive and Records Administration General Records Schedule.
 - (4) A method of isolating the internal DOE network from the SIPRNet, such as using a firewall, must be considered as a boundary protection service. Before RD is transmitted via SIPRNet from an NNSA individual to a recipient internal to NNSA/DOE, the sender must verify the recipient has the appropriate final Access Authorization, such as the appropriate security clearance level, need-to-know, and access briefing (if applicable). The NNSA user must record and retain verification data of the recipients.
- d. Before RD is transmitted via SIPRNet from an NNSA individual to a recipient external to NNSA/DOE, the sender must verify that the recipient has the appropriate final Access Authorization, such as a security clearance, need-to-know, and access briefing (if applicable). The NNSA user must record and retain the verification data of the recipients.
- e. The individual sending the data must ensure that RD to be transmitted via SIPRNet has been reviewed for sensitivity, such as classification level and category, and appropriately marked in accordance with NNSA/DOE policies prior to transmission.
- f. NNSA elements shall ensure that RD is transmitted only as an encrypted attachment to an e-mail. In addition, all data must be encrypted with a NSA type 1 encryption technology.

- g. RD must not be transmitted in the body of an e-mail.
 - h. The responsible Designated Approving Authority (DAA) must accredit the SIPRNet Controlled Interface. Information systems that provide communication with or connectivity to SIPRNet may not connect to any other site network without the approval of the DAAs for the SIPRNet system(s) and site network.
6. CONTACT. Questions concerning this NAP should be directed through the cognizant DAA to the NNSA Cyber Security Program Manager (CSPM), at 301-903-2425.



THOMAS P. D'AGOSTINO
Administrator

APPENDIX A
CONTRACTOR REQUIREMENTS DOCUMENT

This Contractor Requirements Document (CRD) establishes the requirements for National Nuclear Security Administration (NNSA) contractors with access to NNSA and Department of Energy (DOE) information systems. Contractors must comply with the requirements listed in the CRD.

The contractor will ensure that it and its subcontractors cost-effectively comply with the requirements of this CRD.

Regardless of the performer of the work, the contractor is responsible for complying with and 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 doing so, the contractor must not unnecessarily or imprudently flow down requirements to subcontractors. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

1. A plan for the implementation of NNSA Policy Letter (NAP) 14.3-B must be completed within 60 days after modification of the site's contract to include this NAP. The implementation plan shall not exceed three years from the date of formal approval. Further, all information systems as defined in NAP 14.1-C must be protected in accordance with the requirements set forth in NAP 14.3-B. The implementation plan must describe, at a minimum, the program activity to be modified and/or created; the starting date of revision and/or development; the estimated due date; and the responsible party for the stated activity.
2. RD, except for Sigmas 14, 15, 20, and Top Secret, may be transmitted via Secret Internet Protocol Router Network (SIPRNet) from a system that has been formally accredited to process, store, and transmit this RD information.
3. The requirements and implementation of this NAP must be merged into the Information System Security Plan (ISSP) with those of DOE M 205.1-4, Attachment 1 and be subjected to the NNSA Certification and Accreditation process. The ISSP will describe the technical and procedural agreements required for transmission, including clearance and briefings required for access to specific classification levels and categories of information, between the NNSA system and SIPRNet. The test and evaluation of the interconnection must be part of the Security Test and Evaluation Plan of the Certification and Accreditation process.
4. Before RD is transmitted via SIPRNet from an NNSA individual to a recipient internal to NNSA/DOE, the sender must verify the recipient has the appropriate final Access

Authorization, such as a security clearance, need-to-know, and access briefing (if applicable). The NNSA user must record and retain the verification data of the recipients.

5. Before RD is transmitted via SIPRNet from an NNSA individual to a recipient external to NNSA/DOE, the sender must verify the recipient has the appropriate final Access Authorization, such as a security clearance, need-to-know, and access briefing. The NNSA user must record and retain the verification data of the recipients.
 - a. The Access Authorization process, need-to-know, and access briefings, must be validated; however, policy does not authorize the sender and/or DOD recipients to validate their own information.
 - b. These authorizations must be re-validated at least monthly to ensure that each remain current.
 - c. Processes must be established to ensure:
 - (1) A review of at least 20% of the e-mail, including attachments, transmitted and/or received via this controlled interface to ensure that the e-mail does not contain RD that is unencrypted
 - (2) That all RD transmittals have been properly marked. Refer to the User Group Control Memo, dated January, 2006.
 - (3) Records of RD traffic must be maintained, in accordance with DOE records and the National Archive and Records Administration General Records Schedule.
 - d. A method of isolating the internal DOE network from the SIPRNet, such as usage of a firewall, must be considered as a boundary protection service.
6. The individual sending the data must ensure that RD to be transmitted via SIPRNet has been reviewed for sensitivity, such as the classification level and category, and appropriately marked in accordance with NNSA/DOE policies prior to transmission.
7. NNSA elements must ensure that RD is transmitted only as an encrypted attachment to an e-mail.
8. RD must not be transmitted in the body of an e-mail.
9. The responsible DAA must accredit the SIPRNet Controlled Interface. Information systems that provide communication with or connectivity to SIPRNet may not connect to any other site network without the approval of the DAAs for the SIPRNet system(s) and site network.