National Nuclear Security Administration

NNSA **Policy Letter: NAP-14.13**
Date: April 5,
2006

TITLE: Transmission of Restricted and Formerly Restricted Data Over the Secret Internet Protocol Router Network (SIPRNet)

1. OBJECTIVE. To establish requirements and responsibilities for operation of a particular SIPRNet Controlled Interface for the electronic transmission of Restricted Data (RD) and Formerly Restricted Data (FRD) on National Nuclear Security Administration (NNSA) information systems.

2. APPLICABILITY. This NNSA Policy (NAP) applies to all entities, Federal or contractor, that collect, create, process, transmit, store, or disseminate information 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 information system that collects, creates, processes, transmits, stores, and disseminates unclassified or 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," Target of Evaluation (TOE), 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 NNSA or DOE.

   c. Contractors. Except for the exclusions in paragraph 2e, the Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this policy that will apply to contractors whose contracts include the CRD.

      (1) The CRD must be included in site/facility management contracts that provide automated access to NNSA information systems.

      (2) As the laws, regulations, and DOE and NNSA directives clause of site/facility management contracts states, regardless of the performer of the work, site/facility management contractors with the CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD.

(a) 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 Chapter E, Attachment 1, NAP-14.1-A, *NNSA 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.

3. CANCELLATIONS. None.

4. RESPONSIBILITIES. Roles and responsibilities for all activities in the NNSA PCSP are described in NAP-14.1-A, *NNSA Cyber Security Program.*

5. REQUIREMENTS.

a. Restricted Data (RD) or Formerly Restricted Data (FRD), except for Sigmas 14 and 15 and Top Secret, may be transmitted via SIPRNet from a system that meets the Protection Profile (PP) requirements for the Information Group for the RD/FRD information.

b. Before RD/FRD is transmitted, via SIPRNet, from an NNSA, individual to a recipient internal to NNSA/DOE, the sender must verify with the recipient, that the recipient has the appropriate final Access Authorization (security clearance), need-to-know, and access briefing (if applicable). The NNSA user must record and retain the verification data of the recipients.

c. The requirements and implementation of this NAP must be merged with those of the applicable PP, in a System Security Plan (SSP) for the information system, and be subjected to the NNSA Information System Certification and Accreditation Process. The SSP will describe the technical and procedural agreements, including clearance and briefings required for access to specific classification level and category of information, between the NNSA system and SIPRNet. The test and evaluation of the interconnection must be part of the certification process.

d. Before RD/FRD is transmitted, via SIPRNet, from an NNSA individual to a recipient external to NNSA/DOE, the sender must verify with the recipient, that the recipient has the appropriate final Access Authorization (security clearance), need-to-know, and access briefing, NNSA users must record and retain the verification data of the recipients (See 5.h. below).

e. The individual sending the data must ensure that RD/FRD to be transmitted via SIPRNet has been reviewed for sensitivity (classification level and category) and appropriately marked in accordance with NNSA/DOE policies prior to transmission.

f. NNSA elements must ensure that RD/FRD is transmitted only as an encrypted attachment to an email. The attachment must be encrypted using an encryption algorithm that is compatible with the DOD algorithm of the user authorized to receive the RD/FRD attachment.

g. RD/FRD must not be transmitted in the body of an email.

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 DAA responsible for the SIPRNet system and the DAA responsible for the site systems being connected to the SIPRNet system.

6. CONTACT. Questions concerning this NAP should be directed to the NNSA Cyber Security Program Manager, through the cognizant Cyber Security Office Manager, at 301-903-2425.

BY ORDER OF THE ADMINISTRATOR:

Linton Brooks
Administrator

This page intentionally blank.

ATTACHMENT 1

CONTRACTOR REQUIREMENTS DOCUMENT

This Contractor Requirements Document (CRD) establishes the requirements for National Nuclear Security Administration contractors, with access to NNSA and 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.

a. 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 if it is not implemented within 60 days.

b. Restricted Data (RD) or Formerly Restricted Data (FRD), except for Sigmas 14 and 15and Top Secret, may be transmitted via SIPRNet from a system that meets the Protection Profile (PP) requirements for the Information Group for the RD/FRD.

c. Before RD/FRD is transmitted, via SIPRNet, from an NNSA individual to a recipient internal to NNSA/DOE, the sender must verify with the recipient, that the recipient has the appropriate final Access Authorization (security clearance), need-to-know, and access briefing (if applicable). The NNSA user must record and retain the verification data of the recipients.

d. The requirements and implementation of this NAP must be merged with those of the applicable PP, in a System Security Plan (SSP) for the information system, and be subjected to the NNSA Information System Certification and Accreditation Process. The SSP will describe the technical and procedural agreements, including clearance and briefings required for access to specific classification level and category of information, between the NNSA system and SIPRNet. The test and evaluation of the interconnection must be part of the certification process.

e. Before RD/FRD is transmitted, via SIPRNet, from an NNSA individual to a recipient external to NNSA/DOE, the sender must verify with the recipient, that the recipient has the appropriate final Access Authorization (security clearance), need-to-know, and access briefing, NNSA users must record and retain the verification data of the recipients (See 5.h. below).

f. The individual sending the data must ensure that RD/FRD to be transmitted via SIPRNet has been reviewed for sensitivity (classification level and category) and appropriately marked in accordance with NNSA/DOE policies prior to transmission.

g. NNSA elements must ensure that RD/FRD is transmitted only as an encrypted attachment to an email. The attachment must be encrypted using an encryption algorithm that is compatible with the DOD algorithm of the user authorized to receive the RD/FRD attachment.

h. RD/FRD must not be transmitted in the body of an email.

i. 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 DAA responsible for the SIPRNet system and the DAA responsible for the site systems being connected to the SIPRNet system.