



## 1. When are enhanced information system (IS) security controls required on system connections?

Enhanced controls are those controls that are based on contractual requirements, requirements by a Government Contracting Activity (GCA)-sponsored circuit connection or an endorsement by management.

### Systems requiring enhanced controls

Below are some examples of systems that require enhanced controls when your facility's information systems connect to them.

*(Note: This is not a comprehensive list of all systems requiring enhanced controls.)*

- Secret Internet Protocol Router Network (SIPRNet)
- Defense Advanced Research Projects Agency Network (DARPA Net)
- Missile Defense Agency Classified Network (MDACNet)
- Secret Defense Research Engineering Network (SDREN)

## 2. What are examples of enhanced controls?

Below are some examples of both technical and procedural enhanced controls that could apply to your system connections.

*(Note: This is not a comprehensive list of all enhanced controls. This list may be updated as new directives are applicable.)*

### Technical controls:

- Computer Network Defense Service Provider (CNDSP)
- Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIG)— for example,
  1. Network – Enclave, Network Policy, Firewall/Intrusion Detection System (IDS), Network Infrastructure
  2. Operating System(s) as applicable
  3. Host Based Security System (HBSS)
  4. Traditional/Physical Security
  5. Others as applicable; Web, Database, MS Office, Exchange, Internet Explorer etc.
- Host Based Security System (HBSS) OPORD 12-1016
- Defense Security Service (DSS) Communications Tasking Order (CTO) 10-133, Removable Media Guidance
- Vulnerability Scanning (e.g. ACAS)
- SIPRNet Hardware Token
- SIPRNet GIAP System (SGS) registration/maintenance (TO 12-1212)

### Procedural controls:

- DoD warning banner and IS user agreements (CTO 08-008A)
- Insider Threat Mitigation (TASKORD) 13-0651/14-0185)
- Continuity of Operations Plan (COOP), Incident Response Plan , Emergency Destruction Plan
- Configuration/Change Management Plans
- Local IA-related policies and procedures (such as firewall maintenance, IDS/audit reviews)
- Appointment letters for security staff members [such as System Administrators, Information System Security Managers (ISSM), Information System Security Officers (ISSO)]

### 3. How are enhanced controls applied?

To comply with enhanced control requirements, a facility must work with its Government Contracting Activity (GCA) to determine the nature and extent of the additional controls, how these controls must be applied, and how they must be monitored and maintained.

Enhanced controls that must be applied to the system/network, as well as any additional services that must be in place to allow a secure connection, are identified within contract language by a Memorandum of Understanding or Agreement (MOU/A) or by an Interconnection Security Agreement (ISA) with the connecting Authorizing Official/Designated Approving Authority (AO/DAA) and the GCA as signatories.

### 4. What is an example of enhanced controls for a particular system?

Here is an example of SIPRNet enhanced controls:

As a result of the DISA DSS MOA, NISP contractors with DoD Chief Information Officer (CIO) approval to connect information systems to the SIPRNet are required to implement technical applicable SIPRNet DoD IA standards and policies throughout the system's lifecycle.

### 5. What policy requires these enhanced controls?

#### **National Industrial Security Program Operating Manual (NISPOM, 8-610 (a)(1)(e), Connections to Separately Accredited Networks and Systems:**

When connections to other systems exist, a memorandum of understanding is necessary if the systems are approved by a person other than the Cognizant Security Agency (CSA) responsible for this system. A copy of any memoranda of understanding with other agencies shall be attached to the Systems Security Plan (SSP).

#### **Industrial Security Field Operations (ISFO) Process Manual, para 8.0:**

Enhanced controls are those controls that exceed NISPOM requirements. Situations that require enhanced controls are based on contractual requirements, requirements by a GCA sponsored circuit connection (SIPRNet, SDREN, DISN-LES, etc.), or an endorsement by management.

### 6. How do I obtain the tools required for enhanced controls?

NISP contractors with connections to government networks as stated above shall coordinate with the sponsor of the system/network connection to obtain guidance, procedures, and any related tools for implementing the enhanced controls.

#### **Cybersecurity Toolkit – Enhanced Controls**

<https://www.cdse.edu/Training/Toolkits/Cybersecurity-Toolkit/>