Chapter II

Minimum Requirements
for
System Security

As established in this chapter, the general standards, the system security requirements for automated data processing systems (hereinafter referred to as the system), and the criteria for evaluating a system´s ability to protect intelligence information will be uniformly applied throughout the NFIB Community.

II.1. General Security Standards

II.1.a. Information System Security Officer - An Information System Security Officer (ISSO) will be appointed for each ADP system processing intelligence information. The ISSO is responsible for ensuring compliance with the security standards established in this Regulation as well as the implementing directives promulgated by the responsible authority. The ISSO will monitor any changes in system operation that may affect the security status of the total system, report major security deficiencies in system operation, and provide system accreditation statements and recommendations to the responsible authority.

II.2. Personnel Security

II.2.a. When a system is approved to process collateral information up to but excluding Top Secret, all personnel requiring unescorted access to either the central computing facility or the magnetic media storage facility must have a valid security clearance for the security classification level of the collateral information being processed by the system. All personnel requiring unescorted access to a remote terminal/terminal area must have a valid security clearance for the highest security classification of the information designated for input/output at the assigned terminal.

II.2.b. When a system is approved to process Top Secret collateral intelligence information, all personnel requiring unescorted access to either the central computing facility or magnetic storage facility must have a valid Top Secret clearance, and all personnel requiring unescorted access to a remote terminal/terminal area must have a valid security clearance for the highest security classification of the information accessible through the assigned terminal

II.2.c. When a system is approved to process Sensitive Compartmented Information (SCI), all personnel requiring unescorted access to the central computing facility or magnetic media storage facility must be security approved in accordance with DCID 1/14 and have formal access approval for each SCI program being processed by the system, and all personnel requiring unescorted access to a terminal/terminal area must be security approved for the highest security classification of information accessible through the assigned terminal.

II.3. Administrative

II.3.a. All system users must be briefed on the need for exercising sound security practices to protect the intelligence information processed by the system. Users will be informed of the security classification level at which the system is operating and the security requirements for that level.

II.3.a. The processing of intelligence information at any level requires that the Need-to-Know criteria be rigidly enforced. That is, even though all personnel are appropriately cleared, not all personnel shall automatically have authorization to see or use all of the data being processed.

II.3.b. Approval for unescorted visits to a system approved to process intelligence information will be requested in advance via appropriate command channels. In all cases, the request must indicate that the person to make the visit possesses a valid security clearance, is access approvable for any SCI data being processed, and has an established need-to-know.

II.3.c. Administrative approvals (i.e., those not requiring substantive briefings) may be used to grant persons escorted access to the central computing facility and remote terminal areas when, and only when, such persons do not require access to the intelligence information being processed.

II.4 Physical Security

II.4.a. When used for the processing of collateral intelligence information the central computing facility and any remote terminal areas must be secured in a manner commensurate with the classification of the information being processed by the system.

II.4.b. When used for the processing of Top Secret and/or SCI intelligence information, the central computing facility and any remote terminal areas must be secured in accordance with the provisions of USIC Physical Security Standards for SCIFS, NFIB/NFIC-9.1/47.

II.5. Communications Security. - Communications links used to transmit intelligence information between system components or systems must be secured in accordance with appropriate communications security directives for the security level and SCI control channel(s) of the information designated for transmission.

II.6 Emanations Security - The vulnerability of a specific system's operation to exploitation of compromising emanations must be determined during system configuration. For new procurements, guidance on equipment TEMPEST characteristics should be obtained from the appropriate communications security office, and equipment known to have acceptable TEMPEST profiles should be selected. During the system accreditation process, appropriate communications security directives will be implemented for all security elements.

II.7. System Acquisition - Secure system criteria required to meet the general security standards and system security requirements set forth in this Regulation, or system features/capabilities available from advanced state-of-the-art technology, will be included as mandatory in procurement requests for all new systems which will process or handle intelligence information. Vendor submissions for either the development of integrated systems or the delivery of hardware systems must include a review of how the system satisfies the security-related specifications included.

II.8. Systems Maintenance

II.8.a. All vendor maintenance personnel who service automated systems used for the processing of intelligence information shall possess a security clearance commensurate with the highest classification level of the information being processed and access approvable for all SCI being processed.

II.8.b. All uncleared vendor maintenance personnel will be monitored at all times by a system knowledgeable individual possessing a valid security clearance and access approvals for the highest security classification and SCI control channel(s) of the information being processed.

II.8.c As a rule, the use of remote diagnostic links for the maintenance of systems processing classified intelligence information is prohibited. The NFIB member may, however, grant exceptions on a case-by-case basis provided all channels to data storage devices are disabled, internal memory and memory buffers are cleared (both before and after the use of the diagnostic capability), and a separate operating system is used during the diagnostic procedure.

STAT

Page Denied

Next 10 Page(s) In Document Denied