INTELLIGENCE COMMUNITY DIRECTIVE

706

Security Standards For Protecting Domestic IC Facilities

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order 12333, as amended; and other applicable provisions of law.

B. PURPOSE

1. This Directive implements current federal security standards and processes as the baseline for the Intelligence Community (IC) in planning and designing new facilities and renovation of existing facilities. Implementation of the standards and processes identified in this Directive is designed to mitigate security risk to an acceptable level in the construction and protection of domestic IC facilities funded by the National Intelligence Program.

2. This Directive promotes efficient and reciprocal use of IC domestic facilities. It ensures major construction costs are not unnecessarily encumbered by overly stringent security standards.

3. This Directive authorizes the establishment of an IC working group to provide strategic oversight for adherence to and compliance with existing federal domestic physical security standards and processes for the IC in planning and designing new facilities, as well as renovating and modernizing existing federally owned or federally leased facilities.

C. APPLICABILITY

1. This Directive applies to the IC, as defined by the National Security Act of 1947, as amended, and to such elements of any other department or agency as may be designated an element of the IC by the President, or jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned.

2. This Directive applies to new and existing domestic IC facilities, whether owned or leased. IC facilities shall meet the standards referred to in this Directive to the greatest extent possible, with the exception of:

a. IC facilities under construction beyond the 35 percent design phase on the effective date of this Directive.

b. Facilities under leasing action (Solicitation for Offer) as of the effective date of this Directive.

D. POLICY

1. The protection of facilities is a preeminent concern for the IC. Applying baseline physical security standards to manage risks and mitigate threats enables the IC to effectively protect facilities and reduce vulnerabilities.

2. Within the IC, a working group shall assist in the implementation of domestic IC facility security standards.

3. The baseline for IC physical security standards includes a documented risk assessment and a facility protection plan. Risk assessments shall be conducted and protection plans shall be developed, maintained, and executed by IC elements in accordance with standards identified below:

a. Department of Defense (DoD) component IC facilities located on a military installation, as defined by the Secretary of Defense, shall comply with the DoD *Unified Facilities Criteria* (UFC) system as prescribed by MIL-STD 3007 and any other DoD policy including DoD Instruction 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board*, which provides planning, design, construction, sustainment, restoration, and modernization criteria for facilities located on military installations.

b. Non-DoD component IC facilities located on a military installation shall comply with the Department of Homeland Security (DHS), Interagency Security Committee (ISC) Standard: *The Risk Management Process for Federal Facilities*: *An Interagency Security Committee Standard*, and any successor standards.

c. IC facilities not located on a military installation shall comply with the DHS, ISC Standard: *The Risk Management Process for Federal Facilities*: *An Interagency Security Committee Standard*, and any successor standards.

d. Industrial Control Systems (ICS), as defined in the National Institute of Standards and Technology (NIST) Special Publication 800-82, *Guide to Industrial Control Systems Security* shall be protected against unauthorized access. Risks and protective countermeasures shall be identified using the DHS Cyber Security Evaluation Tool (CSET), or accepted alternative software tools. The IC element head or designee shall verify implementation of identified countermeasures and a continuous monitoring plan. Standards to ICS Security or other federal industrial control system standards include, but are not limited to, UFC and/or ISC standards for Industrial Control Systems security.

4. IC facilities shall comply with the appropriate physical security standards identified in Sections D.3.a. through D.3.c. (as applicable) and D.3.d. except where that compliance would jeopardize intelligence sources and methods.

5. Existing IC government-owned facilities shall be brought into compliance with appropriate standards identified in Sections D.3.a. through D.3.c. (as applicable) and D.3.d. within two years of the effective date of this Directive.

6. Existing IC government-leased facilities shall be brought into compliance with appropriate standards identified in Sections D.3.a. through D.3.c. (as applicable) and D.3.d. as soon as possible, but no later than five years from the effective date of this Directive.

7. All facilities shall be constructed, operated, and maintained for reciprocal use by IC elements.

8. IC elements shall maintain appropriate documentation of compliance with standards based on guidance developed by the IC working group established under Section B.3.

E. IMPLEMENTATION

1. Before undertaking any new construction, facility purchases, leasing arrangements, or facility upgrades/renovations, IC elements shall:

a. Coordinate with their respective counterintelligence and security elements consistent with policy outlined in ICD 700, *Protection of National Intelligence*.

b. Consult with appropriate security elements to ensure facility planning and designs incorporate standards identified in Sections D.3.a. through D.3.c. (as appropriate) and D.3.d. of this Directive.

2. Compliance with this Directive is achieved upon completion of a formal risk assessment which includes an acceptance of risk statement from the head of the IC element or designee and an action plan to address areas not meeting UFC or ISC standards. If compliance with standards will jeopardize intelligence sources and methods as identified in section D.4. of this Directive, it shall be noted in the formal risk assessment.

3. Risk assessments and facility protection plans shall be reported by the head of the IC element or designee to the co-chairs of the working group identified in Sections B.3. and D.2. of this Directive.

F. ROLES AND RESPONSIBILITIES

1. The Director of the National Counterintelligence and Security Center (D/NCSC) shall:

a. Co-chair the working group identified in Sections B.3., D.2., and E.3. with the Assistant Director of National Intelligence for Acquisition, Technology & Facilities (ADNI/AT&F).

b. Provide administrative support to the working group.

c. Provide oversight with ADNI/AT&F for compliance with this Directive.

d. Develop additional guidance and standards to effectively implement this Directive.

2. ADNI/AT&F shall:

a. Co-chair the working group identified in Section B.3., D.2., and E.3.with the D/NCSC.

b. Provide oversight with D/NCSC for compliance with this Directive.

c. Update the IC Facilities Management Strategy to ensure consistency with this Directive.

d. Ensure IC element facility standards meet the intent of the IC Facilities Management Strategy.

e. Maintain the central repository of IC facilities.

3. Heads of IC elements shall:

a. Identify, prioritize, assess, and remediate security issues for their respective facilities. Risk management and countermeasures shall be addressed in IC element plans.

b. Utilize appropriate standards (identified in Sections D.3. and D.4. of this Directive) to define the protection criteria and to determine facility security requirements.

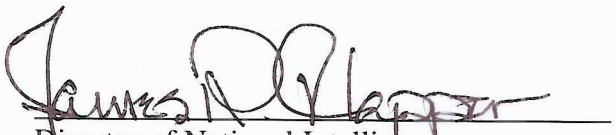
c. Coordinate and communicate facility protection plans with other IC elements entering into facility co-utilization agreements.

d. Report facility documentation and changes to the ODNI in accordance with Section E.3. of this Directive.

e. Appoint a senior-level representative, with management or oversight responsibility of major IC facilities, to the IC working group who can fully and substantially support the group's co-chairs in the execution of his or her responsibilities.

f. Ensure personnel are trained on the standards identified in Sections D.3.a., D.3.b., D.3.c., and D.3.d. as appropriate.

G. EFFECTIVE DATE: This Directive becomes effective on the date of signature.



Director of National Intelligence

16 JUNE 2016

Date