INTELLIGENCE COMMUNITY STANDARD

706-01

18 June 2019

Domestic Facility Security Risk Assessments Standards

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; ICD 706, *Security Standards for Protecting Domestic IC Facilities*; and other applicable provisions of law.

B. PURPOSE: This Intelligence Community Standard establishes security risk assessment standards that apply to domestic Intelligence Community (IC) facilities[1] to promote efficient and reciprocal use and to ensure construction costs are not unnecessarily encumbered by overly conservative security standards.

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

D. RECIPROCITY:

1. IC facilities that have been approved by one IC element head or designee shall be reciprocally accepted for co-utilization by all other elements (i) when there are no deviations from Department of Defense (DoD), *Unified Facilities Criteria* (UFC), or Interagency Security Committee (ISC) Standard, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (ii) or in cases of significant risk acceptance associated with UFC or ISC standards.

2. When an IC facility is being considered for reciprocal use, the "owning" IC element shall share all deviations or risk acceptance decisions with the IC element(s) desiring co-utilization of the facility.

3. IC elements engaged in facility co-utilization should enter into agreements to outline unique responsibilities associated with the co-utilization.

E. FACILITY PLANNING, DESIGN, AND CONSTRUCTION:

1. IC elements shall establish procedures to implement the security provisions of the UFC and/or ISC standards.

2. IC elements shall establish a planning team to oversee the planning, design, construction and occupation of new facilities or major renovations in

[1] IC facilities include any facility, structure or infrastructure, or part thereof for which an IC element has financial or maintenance responsibility.

existing facilities. Planning teams shall establish the design criteria for security and force protection measures that will be built into the facility and will include security and counterintelligence representation. For new construction projects and major renovation projects over 100,000 gross square feet, a blast engineer with formal training in structural dynamics and demonstrated experience with accepted design practices for blast resistant design must be included as a member of the design team, as well as cybersecurity building control systems experts and intrusion detection system experts.

3. The planning team shall ensure the application of analytical risk management, operations security (OPSEC), and security in-depth when planning, designing and constructing IC facilities.

a. Analytical risk management is the process of assessing potential threats against vulnerabilities and implementing security enhancements to achieve protection of assets at an acceptable level of risk and within acceptable costs.

b. OPSEC is a process of denying potential adversaries information about capabilities and intent by identifying, controlling, and protecting generally unclassified information relating to the planning and execution of sensitive operations.

c. Security in-depth is the acceptance of internal or external factors that enhance the probability of detection before or during actual penetration of the facility by the existence of a layer or layers of security that offer mitigations from risk. Where possible, at least one layer should be implemented to allow for less stringent application of level of protection standards.

4. Construction security requirements shall be incorporated into the planning and design of construction and renovation projects in coordination with the local security element responsible for site security and detailed in a Construction Security Plan (CSP) as defined in IC Directive 705, *Sensitive Compartmented Information Facilities*. Construction security requirements will vary based on the size, complexity, and sensitivity of the project. Construction security requirements shall be incorporated into all contract documentation to ensure security requirements are implemented and appropriately funded.

5. IC facilities shall comply with the levels of protection as dictated in the applicable ISC and UFC standards:

a. Facilities located on a military installation[2] shall follow the Design Basis Threat methodology outlined in Chapter Three of UFC 4-020-01, *DoD Security Engineering Facilities Planning Manual*, to determine the "Asset Value" as it applies to the level of protection.

b. Facilities located off a military installation shall follow the Design Basis Threat methodology as outlined in *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*. The baseline level of protection shall be determined by calculating the Facility Security Level as outlined in Section 4.0 of the ISC standard. Appendixes A and B of the ISC standard shall be used to determine the necessary level of protection for any given facility.

---

[2] The term "military installation" means a base, camp, post, station, yard, center, or other activity under the jurisdiction of the Secretary of a military department or, in the case of an activity in a foreign country, under the operational control of the Secretary of a military department or the Secretary of Defense, without regard to the duration of operational control.

6. When designing IC facilities, the planning team shall use the Design Basis Threat explosive weights as specified in the UFC or *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, unless a higher explosive weight is justified based on the local threat environment, sensitivity of mission or other unique circumstances (e.g., headquarters facility, publicly recognized IC facility that is a location for continuity of operations, has large numbers of personnel, contains watch centers, or has high symbolic value). The Office of the Director of National Intelligence/National Counterintelligence and Security Center shall be notified of all decisions to use a Design Basis Threat Explosive weight that differs from UFC or ISC standards.

7. IC elements shall maintain a continuous review process to evaluate ongoing threats and existing countermeasures at domestic facilities to determine if there have been any changes in the threat environment that would require modification of the facilities' security posture. A comprehensive review shall be completed every five years, at a minimum. Where appropriate, new requirements shall be submitted into the IC element's budget process and temporary mitigations implemented to reduce risk until a permanent solution can be implemented.

8. To ensure uniform application and documentation of UFC and ISC security standards, IC elements shall use an ISC-certified tool or equivalent when conducting facility risk assessments. Approved tools shall be credible, reproducible, and defensible to ensure uniform application of security countermeasures across the IC. These tools shall be used by the IC elements to document the facility risk management process and decisions associated with it. Cognizant Security Authorities (CSA) or designees may determine that operational and mission needs preclude strict adherence to these risk assessment requirements. In these instances, an equivalent risk management process and documentation shall be accomplished in accordance with CSA requirements.

F. DEVIATIONS AND RISK ACCEPTANCE:

1. Compliance with this Standard is achieved upon completion of a formal risk assessment and the IC element Head's acceptance of risk or commitment to implement countermeasures contained in UFC or ISC standards.

2. If an IC element is not willing to accept risk associated with failure to comply with a UFC or ISC standard, the IC element should either address or correct the security concerns or initiate the process of relocating the facility to a location that corrects the identified deficiencies.

G. RESPONSIBILITIES:

1. Heads of IC elements, CSAs, or designees shall:

a. Use approved automated tools to enhance security associated with new construction and facility renovations;

b. Establish an internal approval process for UFC deviations or UFC/ISC risk acceptance;

c. Maintain a central record for all facilities under their authority;

d. Report all facilities and deviations in the ODNI central repository of IC facilities;

e. Ensure personnel are trained in the UFC and/or ISC risk management process as appropriate;

f. Identify security and counterintelligence countermeasures that should be designed into the facility; and

g. Ensure a planning team is established to oversee the planning, design, construction and occupation of new facilities or major renovations.

H. EFFECTIVE DATE: This Standard becomes effective on the date of signature.

Director
National Counterintelligence and Security Center

6·18·19
Date