INTELLIGENCE COMMUNITY STANDARD

706-02

Protecting Mission Critical-Facility Related Control Systems (MC-FRCS) in Mission Critical Facilities (MCF)

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management*; ICD 706, *Security Standards for Protecting Domestic IC Facilities*; and other applicable provisions of law.

B. PURPOSE

1. This Intelligence Community (IC) Standard identifies standards and processes designed to mitigate security risks to an acceptable level in the construction and protection of domestic IC MCFs.

2. The identified requirements and processes shall serve as the baseline for IC element use in planning, designing, or renovating MCFs, to include acquisition or modernization of MC-FRCSs. Consistent standards serve to establish a level of reciprocity amongst the IC, allowing for seamless mission and/or personnel transfer amongst applicable facilities.

3. This Standard promotes efficient and increasing reliability of MC-FRCS infrastructure serving National Security Systems.

C. APPLICABILITY

1. This Standard applies to the IC 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 and the head of the department or agency concerned, as an element of the IC.

2. This Standard applies to all new and existing MCFs.

3. This Standard shall support reciprocity of use when consistently applied across MCFs.

D. GUIDANCE

1. IC elements shall protect all MC-FRCSs as information systems integrated with or into secure facilities.

a. IC elements will determine if any Facility Related Control Systems (FRCS) in or for MCFs under the IC element's purview are mission critical.

b. For those FRCSs determined to be mission critical, the MC-FRCS's security categorization will be determined using Intelligence Community Standard 503-03, *Implementing the Risk Management Framework for Intelligence Community Information Systems.*

23 DEC 2019

(1) The Director of the National Counterintelligence and Security Center (D/NCSC) will issue technical implementation guidelines to identify a required minimum-security controls baseline based on an initial MODERATE/MODERATE/MODERATE security categorization for Confidentiality/Integrity/Availability. The baseline will be consistent with Committee on National Security Systems Instruction (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems*, as required by ICS 503-03, with the addition of select enhancements and priorities for particular control families reflecting National Institute for Standards and Technology (NIST) Special Publication (SP) 800-82, *Guide to Industrial Control Systems Security*.

c. If the MC-FRCS's security categorization is different from the baseline described above, IC elements will include additional required security controls from the baseline into the system's security control selections.

d. The implementation of security controls will be prioritized in accordance with technical implementation guidelines (to be defined in future guidance) to minimize MC-FRCS operational risks.

2. IC elements shall develop implementation plans for protecting identified MC-FRCSs and prioritize MC-FRCSs located within existing IC government-owned facilities before MC-FRCSs located within existing government-leased facilities. IC elements have discretion regarding schedule and methods for bringing their MC-FRCSs into compliance with determined MC-FRCS security categorizations identified in Section D.1.

3. Due to rapidly evolving technology and standards, IC elements shall adhere to IC policy such as DNI Executive Correspondence ES 2017-00043, *Wireless Technology in the Intelligence Community*, Wireless Steering Committee issuances, and subsequent guidance related to information systems using radio frequency or over-air communications/wireless capabilities, and should follow Domestic Physical Security Standards Working Group (DPSSWG) recommendations.

4. As FRCSs evolve to leverage secure wireless technologies, the DPSSWG periodically shall provide technical advice to the D/NCSC, as needed, regarding the use of wireless technologies within MCFs.

E. IMPLEMENTATION

1. Personnel responsible for the operation of FRCSs should establish information sharing relationships with their cybersecurity, counterintelligence (specifically technical surveillance countermeasures and supply chain risk management), and security components within their organizations to keep informed regarding threats, vulnerabilities, and related mitigations to their systems. IC elements should consult with these components prior to undertaking any new construction, facility purchases, leasing arrangements, or facility upgrades/renovations.

2. Compliance with this Standard is achieved upon completion of a formal risk assessment and the IC element's acceptance of risk or commitment to implement countermeasures contained in the Unified Facilities Criteria or Interagency Security Committee standards.

F. ROLES AND RESPONSIBILITIES

1. D/NCSC and the Assistant Director of National Intelligence for Acquisition, Procurement and Facilities (ADNI/AP&F) shall, in consultation with IC Chief Information Officer (CIO) and IC elements, develop and establish technical specifications or guidance to implement this Standard in accordance with ICD 706.

2. The ADNI/AP&F shall:

a. Update the IC Facilities & Logistics Enterprise Strategy to ensure consistency with this Standard, and

b. Consistent with ICD 706, maintain the central repository of MCFs.

3. The DPSSWG shall:

a. Assist in the implementation of this Standard, and

b. Provide technical advice to D/NCSC as needed.

4. Heads of IC elements shall:

a. Identify MCFs;

b. Leverage and apply the IC element's existing set of information security program management controls contained in CNSSI 1253 or subsequent version, to complement the security controls established by D/NCSC;

c. Identify, prioritize, assess, and remediate security issues for their respective MCFs;

d. Develop risk management, mitigation, and countermeasure plans for MCFs;

e. Coordinate and communicate facility security plans with other IC elements entering into facility co-utilization agreements;

f. Appoint technical representatives to the DPSSWG;

g. Ensure facility and security personnel understand the application of this Standard;

h. To the extent possible, procure and leverage MC-FRCSs that are demonstrated to comply with the FRCS security requirements detailed herein and, in the event an MC-FRCS does not comply, mitigate identified security risk(s) accordingly;

i. Comply with the security control baseline referenced in D.1.b.(1) except where that compliance would jeopardize intelligence sources and methods;

j. Comply with ICD 503, and adhere to ICS 503-03 and 502-04, *Information Security Continuous Monitoring of Intelligence Community Information Resources*; and

k. Comply with ICD 731, *Supply Chain Risk Management*, and related policies, in the acquisition or maintenance of MC-FRCS.

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

William Evanina

Director
National Counterintelligence and Security Center

12-23-2018

Date

DEFINITIONS

Facility Related Control Systems (FRCS): Industrial Control Systems that control equipment and infrastructure, to include network connectivity and data transfer, that are part of a facility or structure.

Industrial Control System (ICS): Industrial Control Systems encompasses several types of control systems, including Supervisory Control and Data Acquisition systems, Distributed Control Systems, and other control system configurations such as Programmable Logic Controllers, often found in the industrial sectors and critical infrastructures. An industrial control system consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

Mission Critical Facility (MCF): A domestic IC facility (government-owned or -leased) whose loss or incapacitation would result in the inability to perform a mission essential function.

Mission Critical-Facility Related Control Systems (MC-FRCS): The facility related control systems, and associated network infrastructure, that serve to ensure continuity of mission essential functions, or contain National Security Systems related to an officially assigned agency requirement.

Mission Essential Function: The essential functions directly related to accomplishing the organization's mission as set forth in its statutory or executive charter.

Authorization Boundary: All components of an information system to be authorized for operation by an authorizing official, excluding separately authorized systems, to which the information system is connected.