Department of Homeland Security
DHS Directives System
Directive Number: 034-05
Revision Number: 00
Issue Date: 05/21/2018

CLASSIFIED CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

I. Purpose

This Directive sets the responsibilities and policies for the Department of Homeland Security (DHS) to share classified cybersecurity information under the Classified Critical Infrastructure Protection Program (CCIPP). Executive Order (E.O.) 13691, and amended E.O. 12829, designated DHS as a Cognizant Security Authority (CSA) within the National Industrial Security Program (NISP). E.O. 13691 also designated the National Cybersecurity and Communications Integration Center (NCCIC) as a critical infrastructure protection program through which DHS is required to manage the sharing of classified cybersecurity information under this designated critical infrastructure protection program. The CCIPP is executed under DHS's authority as a CSA under the NISP.

II. Scope

This Directive applies throughout DHS to all federal employees, detailees, and contractors providing support to DHS activities and operations associated with the program.

III. Authorities

A. Title 6, United States Code (U.S.C.),

1. Section 132, "Designation of Critical Infrastructure Protection Program"

2. Section 133, "Protection of Voluntarily Shared Critical Infrastructure Information"

3. Section 148, "National Cybersecurity and Communications Integration Center"

B. Executive Order White House Notice: Approval of the Additional National Industrial Security Program Procedures for Sharing and Safeguarding Classified Information with Certain Private or Other Non-Federal Entities, dated December 28, 2016

1. E.O. 12829, as amended, "National Industrial Security Program," dated January 6, 1993

2. E.O. 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," dated August 18, 2010

3. E.O. 13691, "Promoting Private Sector Cybersecurity Information Sharing," dated February 13, 2015

C. DHS Delegation 00002, "Delegation to the Under Secretary for Management"

D. DHS Delegation 12000, "Delegation for Security Operations within the Department of Homeland Security"

E. DHS Delegation 17001, "Delegation to the Under Secretary for National Protection and Programs"

F. DHS Delegation 17009, "Delegation to the Under Secretary for National Protection and Programs Directorate Regarding Cybersecurity"

G. DHS Directive 121-01, "Office of the Chief Security Officer"

IV. Responsibilities

A. The ***Under Secretary for Management*** provides oversight of security personnel, information technology and communications systems, facilities, property, and equipment as administered by the Chief Security Officer.

B. The ***Under Secretary for Intelligence and Analysis*** is responsible for ensuring that any intelligence information held by DHS, including that which is shared pursuant to the CCIPP, is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods under the National Security Act of 1947.[1] All recipients of intelligence information pursuant to the CCIPP shall follow Intelligence Community directives, policy guidance, standards, and specifications for the protection of classified national intelligence and Sensitive Compartmented Information.

[1] 50 U.S.C. Section 3001 et seq.

C. The ***Under Secretary for National Protection and Programs Directorate*** carries out the functions and duties regarding critical infrastructure and the procedures for handling critical infrastructure information, as administered by the Assistant Secretary for Cybersecurity and Communications.

D. The ***National Protection and Programs Directorate Assistant Secretary for Cybersecurity and Communications***:

1. Establishes a programmatic need for an entity to participate in the CCIPP and periodically validates that programmatic need.

2. Nominates non-federal entities for participation in the CCIPP and forwards the name and contact information of the entity to DHS Office of the Chief Security Officer (OCSO) for processing.

3. Conducts the initial engagement with CCIPP entities to determine they do not have an active Facility Security Clearance issued by another CSA under the NISP.

4. Nominates CCIPP-affiliated persons for security clearances under the CCIPP and provides the nominations to DHS OCSO.

5. Maintains projections on the anticipated number of entities and the expected number of security clearance nominations for up to three years forward.

6. Coordinates with interagency partners regarding the nomination of CCIPP-affiliated persons for security clearances, as needed.

E. The ***DHS Chief Security Officer (CSO)***:

1. Oversees the CCIPP operations.

2. Oversees departmental compliance with applicable laws, regulations, policies, and procedures regarding the safeguarding of classified information under the CCIPP.

3. Oversees existing OCSO framework to process security clearances for individuals nominated under the CCIPP.

4. Establishes and manages a Foreign Ownership, Control or Influence (FOCI) analytical program or enters into an agreement with another federal government entity to conduct FOCI analysis on CCIPP entities and provides reports summarizing the findings.

5. Determines CCIPP entities meet all NISP requirements and that each entity is not under FOCI to a degree inconsistent with the national interests.

6. Establishes or enters into an agreement with another federal government entity to establish a FOCI continuous monitoring capability for entities participating in the CCIPP.

7. Establishes and manages a detailee program at the Defense Security Service, which facilitates coordination on CCIPP issues.

8. Develops or enters into an agreement with another Federal Government entity to develop and maintain a database to provide centralized management of CCIPP records and metrics for the CCIPP program:

9. Establishes or enters into an agreement with another Federal Government entity to establish and manage:

a. An oversight and compliance program to periodically validate the status of the entity's need for access to classified national security information and to ensure it remains in compliance with the security agreement, the requirements established by the CCIPP and the NISP; and

b. A program to provide direct security support for approved CCIPP entities, to ensure that classified information disclosed to entity personnel is protected in accordance with national standards. This support includes recurring security education and training, administrative security management, and the investigation of security incidents.

10. Coordinates with inter- and intra-agency stakeholders regarding investigations, including potential counterintelligence issues.

V. Policy and Requirements

A. It is DHS policy to establish a voluntary program that uses the existing information technology and best practices for the classified sharing and collaboration with federal, state, local, and private entities. This program:

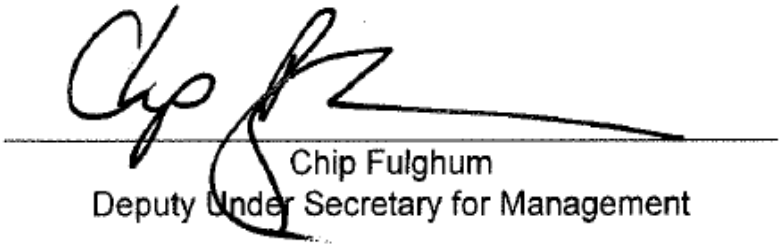
1. Is to establish a community of trust between the Federal Government and entities from across the different critical infrastructure sectors to enable enhanced information sharing and collaboration; and

2. Has participating entities undergo an evaluation to determine whether the company is under FOCI, but they are not required to obtain a Facility Security Clearance.

B. The DHS OCSO issues additional procedures and guidelines regarding the specific requirements for carrying out the responsibilities of this Directive.

VI. Questions

Any questions or concerns regarding this Directive should be addressed to the DHS Office of the Chief Security Officer, National Security Services Division Director.



Chip Fulghum
Deputy Under Secretary for Management

MAY 21 2018
Date