

## **Charter of the Federal Senior Leadership Council**

### **Article I – Establishment and Official Designation**

The National Infrastructure Protection Plan (NIPP) establishes the Federal Senior Leadership Council (FSLC) as one of four principal cross-sector councils.

### **Article II – Mission, Purpose and Scope of Activity**

The purpose of the FSLC is to drive enhanced communications and coordination with respect to critical infrastructure security and resilience matters among Federal departments and agencies that have a role in implementing: (i) the National Infrastructure Protection Plan (NIPP) -- NIPP 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013), (ii) Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience (PPD-21), (iii) Executive Order 13636 - Improving Critical Infrastructure Cybersecurity (EO 13636), and (iv) similar directives and/or subsequently-dated issuances thereof. The FSLC's primary activities include:

- Forging consensus on risk management strategies;
- Evaluating and promoting implementation of risk-informed critical infrastructure security and resilience programs;
- Coordinating strategic issues and issue management resolution among the Critical Infrastructure Cross-Sector Council, the State, Local, Tribal and Territorial Government Coordinating Council, and the Regional Consortium Coordinating Council;
- Advancing collaboration within and across sectors and with the international community;
- Advocating for and tracking execution of NIPP 2013 or subsequently-dated issuances thereof across the Executive Branch;
- Supporting development of resource requests to fulfill the Federal mission; and
- Evaluating and reporting on the progress of Federal critical infrastructure security and resilience activities.

## **Article III – Membership and Member Representatives**

### ***Membership***

The FSLC shall be composed of senior officials who shall have sufficient seniority and authority to make decisions and commit resources on behalf of their departments and/or agencies with respect to the broad range of issues brought before the FSLC (i.e., Principal Representatives). Each of the NIPP Sector-Specific Agencies, for each of its Sectors, and the other Federal departments and agencies assigned critical infrastructure security and resilience responsibilities in PPD-21 listed in Annex A, shall designate two (2) such Principal Representatives. Each Principal Representative will be chosen by its respective Federal department or agency using their own internal procedures.

In the event a Principal Representative is not able to attend a meeting, or otherwise needs to designate a replacement, such designation shall be made on a per-meeting basis only and not for general replacement purposes. The designated replacement shall be able to act with authority at least equal to the authority of the Principal Representative he or she is replacing. The federal department or agency wishing to designate a replacement for a particular meeting shall notify the Cybersecurity and Infrastructure Security Agency, which serves as the FSLC Executive Secretariat, in writing regarding a replacement designation. Such notifications to designate replacement representatives shall be delivered by e-mail to [NIPP@hq.dhs.gov](mailto:NIPP@hq.dhs.gov) prior to the meeting.

## **Article IV – Governance and FSLC Chairperson**

### ***Governance***

The FSLC shall utilize a consultative process, encouraging the exchange of information and points of view, and strive to reach decisions by consensus. The FSLC recognizes that each Principal Representative's Federal department or agency must operate within a mission and parameters that may be distinct from those of the FSLC. At times, a Federal department or agency's mission may restrict a Principal Representative's ability to agree with a potential decision. Under such a circumstance, the Principal Representative should communicate the applicable reasons, justifications, or perspectives clearly to the other Principal Representatives so they may consider the information before reaching a decision. In the event there is dissension, the FSLC Chairperson may, nevertheless, move forward and take such action to fulfill the obligations of the FSLC as long as such action falls within the legal bounds and mandates of the FSLC.

Principal Representatives should represent the positions of their respective Federal government department or agency; however, the FSLC recognizes that Principal Representatives may not always have the legal authority to act on behalf of their Federal department or agency. Therefore, the decisions of individual Principal Representatives are not necessarily binding on any Federal department or agency.

### ***FSLC Chairperson***

FSLC leadership and operation of its meetings shall rest with the Chairperson of the FSLC, which shall be the Director of the Cybersecurity and Infrastructure Security Agency, or his/her designee. The Chairperson shall have the following powers and responsibilities: (i) chairing meetings of the FSLC, (ii) setting FSLC meeting schedules and agendas, (iii) representing the FSLC to the Federal Government and other Critical Infrastructure partners, and (iv) coordinating within the Department of Homeland Security (DHS), the Executive Branch, and the Executive Secretariat.

### **Article V – Meetings**

The FSLC will meet in person or by teleconference on a quarterly basis as a council or in conjunction with the Cross-Sector Councils. Additional meetings and/or conference calls may be scheduled as needed at the Chairperson's discretion or upon request to the Chairperson from a Principal Representative.

### **Article VI – Executive Secretariat and Recordkeeping**

The Cybersecurity and Infrastructure Security Agency will serve as the Executive Secretariat (Secretariat) through staff or contractor support to the FSLC in order to provide meeting logistics, planning, committee and/or working group support and record keeping. The Secretariat will maintain all meeting records, including minutes, in accordance with the records management policy and guidelines established by DHS. The process and procedures for recordkeeping will be described in more detail in the operating procedures applicable to the FSLC.

### **Article VII – Communications**

The FSLC Chairperson shall develop communications and coordination policies and procedures to accommodate its necessary functions. The FSLC is expected to use multiple communications pathways, including e-mail and teleconference platforms, to maintain functionality. In addition, although the FSLC will make all reasonable attempts to arrive at a consensus regarding its recommendations, points of view, and statements, the FSLC will endeavor to relay all significant differing points of view when there is not a consensus opinion.

### **Article VIII – Working Groups, Subcommittees**

The FSLC may form working groups or subcommittees to address certain topics or to undertake substantial or focused investigations, research, or other tasks which cannot be completed during regular FSLC meetings. All subcommittees and working groups shall be subordinate to the FSLC and will report their activities and findings to the FSLC.

## **Article IX – Critical Infrastructure Partnership Advisory Council Relationship**

In the event the FSLC, including its subcommittees and working groups, meets with Sector or Critical Infrastructure Cross-Sector Coordinating Council members or other representative entities of the private sector, those meetings may be designated as Critical Infrastructure Partnership Advisory Council (CIPAC) meetings provided such meetings follow CIPAC compliance procedures.

## **Article X – Duration and Amendments**

The FSLC shall function on a continuing basis for the duration of two years from the signature date. This charter may be modified or amended by consensus of the members.

A handwritten signature in blue ink, appearing to be "C. H. ...", is written over a horizontal line.

Director  
Cybersecurity and Infrastructure Security Agency  
Department of Homeland Security

Date: 3/15/2019



## ANNEX A

### List of Member Agencies and Departments

#### I. Sector Specific Agencies

Chemical: Department of Homeland Security

Commercial Facilities: Department of Homeland Security

Communications: Department of Homeland Security

Critical Manufacturing: Department of Homeland Security

Dams: Department of Homeland Security

Defense Industrial Base: Department of Defense

Emergency Services: Department of Homeland Security

Energy: Department of Energy

Financial Services: Department of the Treasury

Food and Agriculture: Co-Sector-Specific Agencies: Department of Agriculture and  
Department of Health and Human Services

Government Facilities: Co-Sector-Specific Agencies: Department of Homeland Security  
and General Services Administration

Healthcare and Public Health: Department of Health and Human Services

Information Technology: Department of Homeland Security

Nuclear Reactors, Materials, and Waste: Department of Homeland Security

Transportation Systems: Co-Sector-Specific Agencies: Department of Homeland Security  
and Department of Transportation

Water and Wastewater Systems: Environmental Protection Agency

II. Other Agencies and Departments

Department of Commerce

Department of Homeland Security – Office of Policy

Department of Homeland Security – Science and Technology Directorate

Department of Justice

Department of State

Executive Office of the President

Federal Communications Commission

Federal Emergency Management Agency

Nuclear Regulatory Commission

Office of Director of National Intelligence