INTELLIGENCE COMMUNITY POLICY GUIDANCE

404.1

Federal Partner Access to Intelligence Community Information Technology Systems

A. AUTHORITY: The National Security Act of 1947, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004, as amended; Executive Order (EO) 12333, as amended; EO 13618; National Communications System Directive 3-10; and other applicable provisions of law.

B. PURPOSE: This Intelligence Community Policy Guidance (ICPG):

1. Defines the process for Executive agencies or departments that do not contain an embedded Intelligence Community (IC) element, hereinafter referred to as Federal Partners, to access IC information technology (IT) systems containing Sensitive Compartmented Information (SCI) in accordance with Intelligence Community Directive (ICD) 404, *Executive Branch Intelligence Customers*.

2. Sets forth the implementation procedures for Federal Partners to request and gain access to IC IT systems containing SCI information, hereinafter referred to as IC IT systems.

C. APPLICABILITY: This Guidance 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.

D. POLICY

1. The IC shall ensure intelligence information and access to SCI systems and data is provided to authorized Federal Partners and their employees. The process for a Federal Partner and its employees to request access to IC IT systems is identified in Sections E. and F.

2. The DNI has designated the Director, Central Intelligence Agency (D/CIA) to manage the provision of SCI technology connectivity, services, and support for Federal Partners as a service of common concern on behalf of the IC.

3. The DNI, or designee, in consultation with D/CIA, or designee, may waive restrictions on the requirement for the D/CIA to perform this service of common concern if the Federal Partner already has an existing formal relationship with another IC element that provides this service. In such cases, the IC element shall have the same service provider responsibilities as the D/CIA.

E. PROCESS FOR FEDERAL PARTNERS TO REQUEST ACCESS TO IC IT SYSTEMS

1. The Federal Partner, through the Federal Senior Intelligence Coordinator (FSIC), is responsible for identifying a need for access to IC IT systems and for submitting an official request for access to the Assistant Director of National Intelligence for Partner Engagement (ADNI/PE). Federal Partners that do not have a FSIC must use their official representative to the IC to submit the request to the ADNI/PE.

2. The ADNI/PE shall review the official request within 30 days of receipt from the Federal Partner and determine if the requesting agency has sufficient mission need to warrant access to IC IT systems.

3. Provided the ADNI/PE approves the Federal Partner's mission justification for IC IT access, the ADNI/PE shall submit the application to the Information Security Risk Management Committee (ISRMC) and D/CIA, or designee, concurrently. Each entity shall respond to ADNI/PE with their approval or denial within 60 days of receipt of the ADNI/PE's approval of the official request.

a. The ISRMC will review the security of the IC IT system and submit a recommendation to the IC Chief Information Officer (CIO), who will approve or deny the request.

b. The D/CIA, or designee, shall confirm that counterintelligence and physical security standards are met by the Federal Partner in accordance with EO 13526, *Classified National Security Information,* ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information,* and ICD 705, *Sensitive Compartmented Information Facilities*.

4. Provided the D/CIA, or designee, confirms physical security standards are met, including authorizing co-use of an existing SCI facility (SCIF) or creation of a new SCIF, and the IC CIO approves the request, then the application will be forwarded to the ADNI/PE to notify the D/CIA, or designee, to initiate the process for the Federal Partner to receive access to IC IT systems. If the IC CIO or D/CIA, or designee, denies the application, then the Federal Partner will not be granted access to IC IT systems.

5. The ADNI/PE must inform the Federal Partner within 120 days of receipt of the official request if their request was approved or denied.

a. If the ADNI/PE denies the application as discussed in Section E.2., the Federal Partner has the right to appeal the decision to the Deputy Director of National Intelligence for Intelligence Integration (DDNI/II).

b. If the IC CIO denies the application, or D/CIA, or designee, indicates physical security standards are not met, as discussed in Section E.3-4., then the Federal Partner has the right to appeal the decision. A governance board composed of the DDNI/II, IC CIO, and the ADNI/PE, in consultation with CIA as the Cognizant Security Authority in accordance with ICD 703, shall review the official appeal within 60 days of receipt, and all three members of the governance board must approve the application for the Federal Partner to receive access to IC IT systems.

6. Federal Partners that were granted access to IC IT systems prior to the effective date of this Guidance will not need to submit an application via the process outlined in Section E.; however, Federal Partners will be required to submit a renewal application as outlined in Section H.

F. PROCESS FOR EMPLOYEES OF FEDERAL PARTNERS TO REQUEST ACCESS TO IC IT SYSTEMS: The FSIC, or official representative to the IC if the Federal Partner does not have a FSIC, is responsible for nominating to the D/CIA, or designee, their respective agency's or department's employees for access to IC IT systems. The D/CIA, or designee, will approve or deny the request and will verify the applicant has access to SCI and provide network account access within 30 days of receiving the official nomination if the applicant has SCI access. If the applicant does not have SCI access, the applicant must follow the process in ICD 703 and ICD 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information,* to gain access.

G. PROCESS FOR EMPLOYEES OF FEDERAL PARTNERS TO REQUEST ACCESS TO DATA ON IC IT SYSTEMS

1. The Federal Partner and its employees must receive access to IC IT systems prior to receiving access to data on IC IT systems. The originating element will grant or deny access to its data on IC IT systems only after receiving an official request from the FSIC nominating their employees for access to restricted or account-required applications or data.

2. The originating element must receive confirmation from the Federal Partner that all applicable safeguarding requirements in law and policy are met prior to gaining access to the data. These requirements may include classification, privacy requirements, training, or other handling restrictions.

H. PROCESS FOR FEDERAL PARTNERS AND THEIR EMPLOYEES TO RENEW ACCESS TO IC IT SYSTEMS

1. Federal Partners must have their access to IC IT systems renewed every five years. The FSIC shall submit a renewal application to the ADNI/PE, who shall review the mission need, and coordinate with the IC CIO and D/CIA, or designee, to verify the security of SCI networks.

2. Federal Partners that were previously granted access to IC IT networks and did not receive approval from the IC CIO for SCI connectivity must have their renewal application reviewed by the ISRMC and approved by the IC CIO at their first renewal, no later than five years from the effective date of this Guidance, in coordination with the ADNI/PE.

3. Employees of Federal Partners must have their access to IC IT systems renewed every three years, at a minimum, through their employing agency and confirmed by the D/CIA or designee. The FSIC should submit a renewal application to the D/CIA, or designee, who shall review the mission need.

I. PROCESS FOR AUDITING AND MONITORING FEDERAL PARTNERS AND THEIR EMPLOYEES' USE OF IC IT SYSTEMS

1. The D/CIA, or designee, shall:

a. Make available to the Federal Partner audit data on their employees' user activities on IC IT systems as described in Intelligence Community Standard (ICS) 500-27, *Collection and*

Sharing of Audit Data and ICS 700-2, *Use of Audit Data for Insider Threat Detection*. The FSIC, or official representative if the Federal Partner does not have a FSIC, is responsible for ensuring the review of the audit data and the reporting of any violations or abnormalities to the D/CIA or designee;

b. Monitor Federal Partners' compliance with ICD 703, ICD 704, and ICD 705, and report any variance to the ADNI/PE; and

c. Monitor Federal Partners' compliance with ICD 502, *Integrated Defense of the Intelligence Community Information Environment*, and ICD 503, *Intelligence Community Information Technology Systems Security Risk Management*, to include data handling procedures, and report any variance to the ADNI/PE.

2. IC elements shall ensure the monitoring of activities by employees of Federal Partners on the IC element's applications in accordance with Executive Order 13587, "*Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,*" and the Presidential Memorandum, "*National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs,*" and report any variance to the FSIC and the D/CIA or designee. The monitoring may include recurring manual or automated review of content produced, discovered, processed, or received, and shall support insider threat mitigation functions.

J. ROLES AND RESPONSIBILITIES

1. The ADNI/PE shall:

a. Publish the application and renewal forms for Federal Partners and their employees to request access to IC IT systems within 30 days of issuance of this Guidance, and make the application forms readily available to IC elements and Federal Partners;

b. Compile a comprehensive list of all Federal Partners with IC IT system access, update the list annually, and disseminate to IC elements upon request;

c. Compile and retain a comprehensive list of all Federal Partners that requested IC IT access but were denied and update the list annually; and

d. Notify the Federal Partner at least 90 days before their application for renewal of access to IC IT systems is due.

2. The IC CIO shall include data on Federal Partners' use of IC IT systems in their report to the DNI on the status of the integrated defense of the IC information environment as required in ICD 502.

3. The D/CIA, as the provider of this service of common concern, shall:

a. Provide the ADNI/PE an annual list of all the employees of Federal Partners who have been granted or denied access to IC IT systems;

b. Monitor employees of Federal Partners' activities on SCI networks to ensure access is consistent with U.S. legal and policy requirements, and report any variance to the relevant FSIC and ODNI;

c. Establish a memorandum of understanding, reviewed annually, delineating responsibilities performed by CIA and the Federal Partner for IC IT access, and make this document available to IC elements upon request; and

d. In coordination with the ADNI/PE, develop a financial agreement with each Federal Partner that receives IC IT systems based on the services provided, as required.

K. EFFECTIVE DATE: This Policy Guidance becomes effective on the date of signature.

David R. Cohen

Director of National Intelligence

June 16, 2017

Date