FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554	TITLE	
	FCC Insider Threat Program	
FCC DIRECTIVE	**Directive Number:** **FCCINST 1133.2**	**Effective Date:** **April 2020**

TO: All Employees

SUBJECT: Compliance with the FCC Insider Threat Program

1. **Purpose:** This directive establishes policy and assigns responsibilities for the Federal Communications Commission (FCC) to fulfill the requirements of the National Insider Threat Program. This Directive also authorizes issuance of the FCC Insider Threat Implementation Plan (InThIP) containing policies, procedures, roles, responsibilities, and information requirements for implementing the FCC Insider Threat Program. The FCC InThIP will be updated, as necessary, to reflect changes in law, regulation, or Presidential guidance or Executive Order. The FCC InThIP will be protected as Controlled Unclassified Information (CUI), and will be available only to the Managing Director (MD), the Senior Agency Official (SAO), Security Operations Center (SOC), and members of the Insider Threat Working Group (ITWG) on the Insider Threat electronic "Hub."

2. **Cancellation:** This instruction supersedes FCCINST 1133.1 dated August 5, 2016.

3. **Scope and Applicability:** This Directive applies to all FCC Bureaus and Offices (B/Os), as well as staff who hold any level of a National Security Clearance sponsored by the FCC, including Federal employees, contractors, temporary staff, interns, and volunteers.

4. **Authorities:** This Directive is published in accordance with guidance contained in Executive Order 13587 of October 7, 2011, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*. The Executive Order establishes the requirement for federal agencies to develop, implement, and maintain an Insider Threat Program through the National Insider Threat Task Force (NITTF) which is co-chaired by the Attorney General and the Director of National Intelligence.

   Subsequent statutes, executive orders, or regulations which alter the terms of this Directive shall take precedence.

5. **Policy:** An insider threat arises when a person with authorized access to classified U.S. Government resources, including personnel, facilities, information, equipment, networks, and systems, uses that access to harm the security of the United States. The FCC Insider Threat Program's goal is to deter, detect, and mitigate actions by staff who may represent a threat to national security. These threats encompass potential espionage, violent acts against the

Government or the nation, and unauthorized disclosure of classified information including data available on interconnected U.S. Government computer networks and systems.

The FCC Insider Threat Program includes the capability to gather, integrate, and centrally analyze and respond to key insider threat-related information; monitor staff use of classified information systems and material; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel.

6. <u>Responsibilities:</u> Listed below are the major responsibilities for the key positions that oversee the FCC Insider Threat Program. A complete list of roles, responsibilities, policies, procedures for carrying out the program and information regarding deterrence, detection, and mitigation of threats to national security are located in the FCC *InThIP* document.

A. The Managing Director (MD) shall:

1. Oversee the FCC Insider Threat Program and allocate adequate resources to carry out its implementation; and

2. Act as or appoint the Senior Agency Official for the FCC Insider Threat program;

B. The Senior Agency Official (SAO) for the FCC Insider Threat Program shall:

1. Ensure efficient and effective management, accountability, and day-to-day oversight of the FCC's Insider Threat Program, and;

2. Ensure the Chief Security Officer, Security Operations Center (SOC), Administrative Operations (AO) in OMD as the principal lead, carries out the responsibilities and functions of the FCC's Insider Threat Program.

C. The Chief Security Officer, SOC, as principal lead, shall:

1. Carry out the FCC Insider Threat program and make resource, policy, procedure, and process recommendations to the MD/SAO;

2. Serve as the FCC Insider Threat Program Manager (InThPM) and have the Deputy Chief Security Officer serve as the FCC Insider Threat Deputy Program Manager (InThDPM);

3. Serve as the Chair of the FCC Insider Threat Working Group (ITWG) and have the Deputy Security Officer serve as the Deputy Chair of the ITWG;

4. Seek support from owners of Classified networks, per Executive Order 13587 and NITTF, for the technical capability, subject to appropriate approvals, to monitor user activity on all Classified networks in order to detect activity indicative of insider threat behavior;

5. Develop a comprehensive process to gather, integrate, and centrally analyze and respond to counterintelligence, security, information assurance (information technology), human resources, law enforcement, and other relevant information indicative of a potential insider threat;

6. Implement policies and procedures for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel;

7. Maintain a file of non-disclosure agreements signed by all FCC cleared individuals acknowledging that they must adhere to all laws and regulations with respect to protecting Classified information;

8. Maintain a file of agreements signed by all FCC cleared individuals, acknowledging that they have no expectation of privacy with respect to their activity on any agency Classified network, to include portable electronic devices, and that such activity is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding;

9. Ensure that "banners" exist on FCC (subscriber) Classified networks that inform users that they have no expectation of privacy with respect to their activity on such networks, that their activity on such networks will be monitored to ensure that user activity is for lawful U.S. Government authorized purposes, and that misuse and/or compromise of Classified information can result in criminal, security, or administrative actions against the users;

10. Develop guidelines for B/Os to securely, discretely, and in a timely manner, provide the FCC InThPM/InThDPM upon request information necessary to identify, analyze, and resolve insider threat matters;

11. Establish a FCC Insider Threat Working Group (ITWG) comprised of appropriate staff, to include but not limited to individuals from the Office of Managing Director's front office, SOC, Human Resources Management, Information Technology, Office of General Counsel (OGC), and the Public Safety and Homeland Security Bureau (PSHSB), including the Federal Senior Intelligence Coordinator. Upon FCC InThPM/InThDPM request, members of the FCC ITWG will securely, discreetly, and in a timely manner, provide the FCC InThPM/InThDPM information necessary to identify, analyze, and resolve insider threat matters;

12. Ensure that FCC personnel assigned to the ITWG are fully trained in the following: the Insider Threat Program and applicable counterintelligence and security fundamentals; FCC procedures for conducting insider threat response actions; applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information; applicable civil liberties and privacy laws, regulations and policies; and in investigative referral requirements of Section 811 of the Intelligence Authorization Act for FY 1995, as well as

other policy or statutory requirements that require referrals to an internal or external entity;

13. Ensure FCC Insider Threat awareness training is provided and that training course completion is verified for all new cleared and non-cleared employees at entry-on-duty and for all cleared and non-cleared employees annually;

14. Ensure the annual FCC Insider Threat awareness training for all personnel addresses current and potential threats in the work and personal environment and includes, at a minimum, the following topics: the importance of detecting insider threats and reporting suspicious activity to the InThPM/InThDPM, and methodologies of adversaries to recruit trusted insiders and collect Classified information;

15. Establish a secure internal electronic FCC Insider Threat site ("Hub") that is accessible to all FCC cleared individuals and the MD, SAO, SOC, and ITWG. The FCC Hub provides insider threat reference material, including indicators of insider threat behavior, training information, reporting requirements, policy, procedures, roles, responsibilities and a secure means of reporting and reviewing matters of the Insider Threat Program. The electronic Hub is segmented and limits access to the FCC InThIP and specific insider threat information to only the MD, SAO, SOC, and ITWG as necessary. The InThPM/InThDPM is responsible for making all access decisions regarding insider threat information contained in the Hub;

16. Implement oversight mechanisms and/or procedures to ensure proper handling and use of records and data;

17. Limit access as necessary to such records and data to only those staff who require the information to perform their authorized FCC Insider Threat Program function;

18. Ensure adherence to guidelines and procedures for the retention of records and documents necessary to complete assessments required by Executive Order 13587, and NITTF, and;

19. Produce an annual report to the MD, SAO, and NITTF's Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to ensure compliance with the FCC InThIP and the National Insider Threat Program as prescribed by Executive Order 13587 and NITTF.

D. FCC Insider Threat Working Group (ITWG) shall:

1. Provide information to the FCC Chair and FCC Deputy Chair of the ITWG who also serve as the FCC InThPM/InThDPM;

2. Be fully trained in the following: the Insider Threat program and applicable counterintelligence and security fundamentals; FCC procedures for conducting insider

threat response actions; applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information; applicable civil liberties and privacy laws, regulations, and policies; and investigative referral requirements of Section 811 of the Intelligence Authorization Act for FY 1995, as well as other policy or statutory requirements that require referrals to an internal or external. entity;

3. Have appropriate access to the FCC InThIP and insider threat information available at the FCC Hub;

4. Upon FCC InThPM/InThDPM request, securely, discretely, and in a timely manner, provide the FCC InThPM/InThDPM information necessary to identify, analyze, and resolve insider threat matters.

E. FCC Bureaus and Offices shall:

1. Comply with the FCC Insider Threat Program; and

2. Upon request, securely, discreetly, and in a timely manner, provide the FCC InThPM/InThDPM information necessary to identify, analyze, and resolve insider threat matters.

F. Office of the General Counsel shall:

1. Advise and assist on all legal matters related to the administration of the FCC Insider Threat Program;

2. Oversee FCC Insider Threat Program compliance with applicable civil rights, civil liberties, and privacy requirements.

G. All FCC Cleared Individuals shall:

1. Report to the InThPM/InThDPM all contacts, activities, indicators, or behaviors that they observe or gain knowledge of that could adversely impact the responsible sharing and safeguarding of Classified information. A list of reportable contacts, activities, indicators, and behaviors as well as current information materials are available at the FCC Hub and accessible by all FCC cleared individuals.

7. Effective Date and Implementation:

This Directive is effective immediately and shall be implemented promptly upon distribution.

Thomas M. Johnson, Jr.
General Counsel

Mark Stephens
Managing Director