FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 **FCC DIRECTIVE**	**TITLE** **Compliance with the FCC Cyber Security Program**	
	Directive Number: **FCCINST 1479.5**	**Effective Date:** **May 20, 2015**

TO: All Employees

SUBJECT: Compliance with the FCC Cyber Security Program

Purpose. This directive establishes policy and assigns responsibilities for assuring optimal levels of cyber protection required for Federal Communications Commission (FCC) information systems. This Directive also authorizes issuance of the *FCC Cyber Security Policy* program which containing detailed policies, procedures, and information requirements for implementing cyber security controls. The *FCC Cyber Security Policy* will be updated, as necessary, to reflect changes in law, regulation or Presidential guidance or Executive Order.

Scope. This Directive applies to all FCC Bureaus, Offices, and Staff including Federal employees, contractors, temporary staff, interns, and volunteers who access and use FCC information systems to conduct the Commission's business including remote access and use such as while teleworking or on travel.

Authorities. This Directive is covered by numerous Public Laws, Executive Orders, regulations, Presidential Decision Directives, OMB Circulars, and National Institute of Standards and Technology publications among other guidance and authoritative references. A complete and detailed list is located in Appendix C of the *FCC Cyber Security Policy.*

Policy. The FCC's cyber mission is to ensure the security of our information resources, environment and communications to provide a secure, reliable, and resilient platform where both the Commission and the public can access information. The Commission increasingly replies on information technology, specifically the internet, wireless and mobile devices, and data exchange services to conduct its business. Cyber security measures are crucial to ensure the protection and preservation of the confidentiality, integrity, and availability of electronic information resources critical to the FCC, the U.S. Government, and the public.

The *FCC Cyber Security Policy*, incorporated by reference into this Directive, comprises the cyber security management structure and foundation to measure progress and compliance, and is organized into five major sections as follows:

SECTION 1: INTRODUCTION -- This section covers among other items, the information security program, the policy overview, various cyber threats and information technology definitions.

SECTION 2: ROLES and RESPONSIBILITIES -- This sections covers in detail the roles and responsibilities of information security staff, organizations and individuals ranging from the Chairman's position to individual users as addressed under Scope above.

SECTION 3: MANAGEMENT CONTROLS -- These controls focus on managing both system information security controls and system risk. These controls consist of risk mitigation techniques used by management.

SECTION 4: OPERATIONAL CONTROLS -- These controls focus on mechanisms primarily implemented and executed by individuals. Operational controls are designed to improve the security of a particular system or group of systems and often rely on management and technical controls.

SECTION 5: TECHNICAL CONTROLS -- These controls focus on security controls executed by information systems. Technical controls provide automated protection from unauthorized access or misuse; facilitate detection of security violations; and support security requirements for applications and data.

Responsibilities.
Listed below are the major responsibilities for the key positions that oversee FCC information security. A complete list of roles and responsibilities for all information security levels are located in Section 2 of the *FCC Cyber Security Policy* document.

A. The Managing Director is responsible for oversight of the cyber security program and allocation of adequate resources for information system security and shall:

- Appoint the Chief Information Officer (CIO);
- Ensure that an Cyber Security Program is established and managed in accordance with Federal law, regulation, directives and order, and by FCC policy and directives;
- Ensure that Senior officials such as the CIO, Deputy CIO for Resiliency (DCIOR) and Chief Information Security Officer (CISO) are held accountable for data and information systems protection;
- Ensure that the security of information systems is an integral part of the life cycle management process for all information systems developed and maintained;
- Ensure that adequate funding for information security is provided for information

systems and that adequate funding requirements are included for all information systems budgets;

- Ensure that information system data are entered into the appropriate FCC Security Management Tools to support FCC information security oversight and FISMA reporting requirements; and
- Ensure that the requirements for an information security performance metrics program are implemented and the resulting data maintained and reported.

B. The Chief Information Officer is the senior agency executive responsible for all FCC information systems and their security as well as for ensuring FISMA compliance and shall:

- Heads an office with the mission and resources to assist in ensuring compliance with the FCC Information Security Program;
- Oversees the development and maintenance of a Commission-wide information security program;
- Appoints a FCC employee to serve as the DCIOR;
- Appoints a FCC employee to serve as the CISO;
- As appropriate, serves as or appoints a FCC employee to serve as the Authorizing Official (AO) for FCC information systems.
- Participates in developing FCC performance plans, including descriptions of the time periods and budget, staffing, and training resources required to implement the FCC security program;
- Ensures that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with FCC information security policies;
- Ensures that FCC security programs integrate fully into the FCC enterprise architecture and capital planning and investment control processes;
- Ensures that System Owners understand and appropriately address risks, including interconnectivity with other programs and systems outside their control;
- Reviews and evaluates the FCC Cyber Security Program annually;
- Ensures that an information security performance metrics program is developed, implemented, and funded;
- Reports to the FCC Managing Director on matters relating to the security of FCC systems;
- Ensures compliance with applicable information security requirements;
- Coordinates and advocates resources for enterprise security solutions; and
- Leads the FCC Contingency Planning program.

C. The Deputy Chief Information Officer for Resiliency is responsible for all commission information systems and their security as well as for ensuring FISMA compliance and shall:

- Establish and oversee the FCC information security program;
- Direct a review of the information security program plan be performed with a frequency depending on risk, but no less than annually;
- Ensure that information security concerns are addressed at Configuration Control Boards, and throughout the System Development Life Cycle
- Ensure that an accurate information systems inventory is established and maintained;
- Ensure that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with FCC information security policies
- Ensure that System Owners understand and appropriately address risks, including risks arising from interconnectivity with other programs and systems outside their control;
- Ensure that an information security performance metrics program is developed, implemented, and funded;
- Advise the FCC CIO of any issues regarding infrastructure protection, vulnerabilities or the possibility of public concern;
- Ensure that incidents are reported to the Network Security Operations Center (NSOC) within reporting time requirements as defined in *FCC Cyber Security Policy* document;
- Ensure compliance with FCC information systems security policy;
- Coordinate and advocate resources for information security enterprise solutions; and
- Provide the resources and qualified personnel to ensure compliance with FCC security policy.

D. The Chief Information Security Officer is responsible for developing a security strategy and establishing, maintaining, directing and coordinating implementation of the FCC Cyber Security program and shall:

- Ensure that appropriate technical, management, and operational controls are in place for adequately protecting FCC data and information systems, including data stored or used when remotely such as teleworking or traveling on official business;

- Establish a Cyber Security Program that addresses federal statutory and regulatory requirements for the high-level areas;

- Issue agency-wide cyber security policy, guidance, and security architecture requirements for all FCC IT systems and networks, in compliance with the authorities listed in Appendix C of the *FCC Cyber Security Policy* document;

- Serve as the principal agency liaison with organizations outside the FCC for matters relating to cyber security;

- Review and approve the tools, techniques, and methodologies planned for use in applying the Risk Management Framework to FCC IT systems and for reporting and managing systems-level FISMA data, including but not limited to Security Test and Evaluation (ST&E) plans, contingency plans, and security risk assessments;

- Consult with the FCC Chief Security Officer on matters pertaining to physical security, personnel security, investigations, and Top Secret (TS) and Sensitive Compartmented Information (SCI) systems, as they relate to information security and infrastructure;

- Develop and implement procedures for detecting, reporting, and responding to information security incidents;

- Consult with the Office of General Counsel, Office of the Inspector General, and the Office of Managing Director's Human Resources Management to develop and/or update the FCC Computer System User Rules of Behavior (RoB). Work with OMD's Human Resources Management, the Security Operations Center and the Enterprise Acquisition Center, and B/Os to ensure all users read and sign indicating acceptance of the RoB;

- Ensure that all individuals receive security awareness training BEFORE accessing and using the FCC network and information systems;

- Provide oversight and guidance for the FCC Network Security Operations Center (NSOC); and

- Consult with the International Bureau regarding cyber security matters involving international travel and travelers on official FCC business.

E. The System Owners or Technical Stewards are responsible for the successful operation of the information systems and programs within their program area and are ultimately accountable for their security. All systems require a System Owner designated in writing for proper administration of security and shall:

- Ensure that each of their systems is deployed and operated in accordance with the *FCC Cyber Security Policy* document;

- Ensure that an Information System Security Officer (ISSO) is designated in writing for each information system under their purview;

- Ensure only one System Owner designated for each FCC system;

- Ensure information security compliance, development and maintenance of security plans, user security training (if applicable), notifying officials of the need for security authorization and need to resource; and

- Ensure development of a POA&M to address weaknesses and deficiencies in the information system and its operating environment.

F. All Individuals that access and use the FCC network and information systems shall read, sign and follow the FCC Computer User Rules of Behavior.

Jon Wilkins
Managing Director