FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE FCC CYBERSECURITYAND PRIVACY PROGRAM	
	Directive Number: FCCINST 1479.6	Effective Date: April 2022

1. PURPOSE: This directive establishes policy and assigns responsibilities for assuring optimal levels of information security and privacy required for Federal Communications Commission (FCC or Commission) information systems and information technology resources.

2. BACKGROUND: The FCC Cybersecurity and Privacy Program, as defined in this directive and the associated Cybersecurity and Privacy Policy (CSPP), requires the adherence to policies, procedures, and requirements for the implementation of information security and privacy controls. These controls generally protect against potential security vulnerabilities and breaches by providing safeguards to minimize risks to individuals, information systems, physical property, and other assets. This directive will be updated as necessary to reflect changes in relevant federal laws, regulations, guidance, or Executive Orders. The associated policy has been drafted in accordance with the FCC's responsibilities to protect information contained in its information technology systems and will be updated as the security or privacy requirements change in response to new technologies and federal guidance, but not less than annually. The current version of the policy document is available for review on the FCC Intranet.

3. CANCELLATION: This instruction replaces the formerly separate FCCINST 1479.5, dated May 20, 2015, titled "FCC Cyber Security Program."

4. SCOPE AND APPLICABILITY: This directive and the associated policy apply to all FCC Bureaus, Offices, individuals, and staff (i.e., Federal employees, contractors, temporary staff, interns, and volunteers) who access and use FCC information systems or data to conduct Commission business, including remote access and use while teleworking or on travel. This directive and associated policy also apply to all information collected or maintained by, or on behalf of, the FCC and all information systems used or operated by an FCC contractor or any organization on behalf of the FCC.

5. AUTHORITIES: Federal Information Security Modernization Act of 2014, 44 USC 3551, et seq., as amended; Section 208 of the E-Government Act of 2002, 44 U.S.C. 3501

note; the Privacy Act of 1974, 5 U.S.C. 552a; Executive Orders; Office of Management and Budget (OMB) Memoranda and Circulars; and the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications.

6. POLICY: The Commission increasingly relies on information technology, specifically the internet, wireless and mobile devices, and data exchange services to conduct its business. With this directive, the FCC authorizes an overarching Information Security and Privacy Policy in accordance with guidance from the Office of Management and Budget.[1] The purpose of the CSPP is to protect the confidentiality and integrity of information stored and processed in FCC systems, and to ensure that the systems and information are available to authorized users when required. Security and privacy controls are crucial to ensuring the protection and preservation of the Confidentiality, Integrity, and Availability (CIA)[2] of electronic information resources critical to the FCC, the U.S. Government, and the public.

   All FCC information and systems shall be protected from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction, whether accidental or intentional, to maintain the CIA. Security and privacy controls that provide this protection shall meet minimum federal requirements, ensure that FCC information is persistently protected, and promote a defense-in-depth security strategy.

   FCC will follow the NIST Special Publication (SP) 800-37, *Risk Management Framework*, as a starting point that promotes consistent, cost-effective security and privacy standards across all FCC information assets and services. NIST SP 800-53 and OMB guidance are used to establish the security and privacy baselines by defining appropriate security and privacy controls to protect FCC information assets, systems, and services.

   All FCC employees, contractors, and entities with access to federal information systems[3] will abide by all the policies defined within the CSPP and any other applicable documents to ensure CIA of all information systems.

7. ROLES & RESPONSIBILITIES:

   The following is a brief overview of the roles and responsibilities related to information security and privacy at the FCC. A full description of these responsibilities is contained in the CSPP and related policies and directives, including FCCINST1113.2 Compliance with Privacy Laws and Guidance, and the FCC Breach Response Policy.

[1] OMB Circular A-130.
[2] 44 U.S.C. 3552(3); OMB Circular A-130.
[3] Federal information system means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency. *See* Office of Management and Budget (OMB) Circular A-130, "*Managing Information as a Strategic Resource*," August 28, 2016 (OMB Circular A-130) at 29.

A. The FCC Chief Information Officer (CIO) shares overall responsibility for the CSPP with the Senior Agency Official for Privacy, and has primary responsibility for overseeing the development and maintenance of a Commission-wide information security program as set forth in the CSPP.

B. The FCC Senior Agency Official for Privacy (SAOP) shares overall responsibility for the CSPP with the CIO and is primarily responsible for developing, implementing, and maintaining a Commission-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems.

C. The FCC Chief Information Security Officer (CISO) shall carry out the CIO's responsibilities under FISMA,[4] with information security as their primary duty, and shall head a team with the required mission and resources to assist in achieving and maintaining organizational compliance with FCC information security policies, standards and procedures.

D. The FCC Bureau and Office Chiefs are responsible to ensure adherence to security, compliance, and privacy requirements by their staff and for all system(s) managed that support their business missions.

E. The Information (IO) and System Owners (SO) are personnel, IT or non-IT, responsible for managing the lifecycle (i.e., procurement, development, integration, modification, operation, maintenance, and disposal) of a specific system or service and the information it handles.

F. The FCC System Users including staff, contractors, temporary staff, interns, external users, including any external partners or corporations that maintain FCC information, must adhere to agency policies, including those described in section 8 of this Directive, "Rules of Behavior," and staying up to date on changes to those policies and directives.

[4] The Federal Information Security Management Act of 2002, enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002) was subsequently modified by the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014). As modified, FISMA is codified at 44 U.S.C. § 3551 et seq.

8. RULES OF BEHAVIOR (ROB): The Privacy Act of 1974, FISMA, OMB A-123, and OMB A-130 mandate that federal agencies maintain RoB for using federal systems. Prior to providing access to FCC systems, all personnel, including contractors and others working on behalf of the FCC, must agree to the FCC's RoB. The RoB delineate responsibilities and expected behavior of all individuals with access to FCC systems and state the consequences of non-compliance. The CIO, or his/her designee, and the SAOP shall define and maintain enterprise-wide RoB that can be used for all information systems. The RoB shall be reviewed and updated as necessary. FCC IT shall ensure that users requesting access to FCC systems sign the FCC RoB after receiving training on both the RoB and the disciplinary actions that may result if the RoB are violated.

9. PRIVACY REPORTING AND HANDLING: The FCC has established a process for management of breaches, as set forth in the "Breach Response Policy," available on the FCC Intranet. Employees are directed to follow those instructions when appropriate.

10. EFFECTIVE DATE AND IMPLEMENTATION: This directive is effective immediately and shall be implemented promptly upon distribution.

Mark Stephens

Digitally signed by Mark Stephens
Date: 2022.04.21 09:37:41 -04'00'

Mark Stephens
Managing Director