FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE FCC Information Security Program	
	Directive Number: FCCINST 1131.2	Effective Date: June 7, 2013

1. PURPOSE: This directive establishes the policy for the classification, downgrading, declassification, transmission, transportation, and safeguarding of information requiring protection in the interests of national security. It primarily pertains to classified national security information, now known as classified information, but also addresses Controlled Unclassified Information (CUI) as outlined in E.O. 13556. The Federal Communications Commission (FCC) Information Security Manual contains the minimum standards for the protection of classified information and material. Such standards may be enhanced but never lessened as a commission option. This manual also provides guidance on the proper handling of sensitive unclassified material.

2. SCOPE: This directive applies to all FCC employees at headquarters and field units.

3. AUTHORITY: The statutory authority for this program is derived from Executive Order 13526, "Classified National Security Information," and 32 C.F.R., Part 2001, Title 18 of the United States Code, and guidance from the Office of Management and Budget and the National Security Council.

4. POLICY:

   A. All FCC personnel, regardless of position, have a personal and official responsibility for the proper safeguarding and protection of the information to which they have access, particularly classified information.

   B. Information will be categorized as classified or protected as sensitive only when it is in the interest of national security, and downgraded or declassified when it is determined that the information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than is currently required.

   C. Information and material classified under this regulation will be afforded a level of protection against unauthorized disclosure commensurate with the level of classification or sensitivity assigned. Responsible officials will ensure that classified and sensitive information and materials are adequately protected from compromise.

D. Access to classified information is authorized only to the following personnel:

(1) Persons with the appropriate need-to-know in order to perform a lawful and authorized governmental function;

(2) Persons who have been granted a security clearance and access authorization at the appropriate level of clearance.

(3) Persons who have executed an appropriate non-disclosure agreement. The FCC Personal Security and Suitability Manual contains policy on the personnel security clearance program. The holder, not the potential receiver of the information, determines the need-to-know and is responsible for verifying the clearance and access authorization of the potential receiver. No person will be granted access to classified information solely by virtue of their position.

E. Classified and sensitive information will be maintained only when necessary for the operation of the organization or when law, regulation, or records management policy requires its retention.

5. RESPONSIBILITIES:

A. FCC Chairman. The FCC Chairman shall

(1) appoint a senior agency official to be responsible for direction and administration of the program within the FCC. This position will be the Security Officer for the FCC and hold the position title of Manager, Security Operations.

(2) commit necessary resources to the effective implementation of the information security program.

B. Managing Director. The Managing Director will

(1) designate a Commission Security Officer (CSO) by written appointment. The CSO will be of sufficient grade to effectively discharge assigned duties and responsibilities. The CSO will have direct access to the Managing Director and the FCC Chairman on matters affecting the information security program.

(2) ensure adequate funding and resources are available to allow security management personnel to manage and administer applicable information security program requirements.

(3) ensure the CSO is afforded security training consistent to the duties assigned.

C. Commission Security Officer. The CSO is the principal advisor on information security in the commission and is responsible to the OMD and Chairman for management of the program. The CSO will

(1) advise and represent the Managing Director and the FCC Chairman on matters related to the classification, downgrading, declassification, and safeguarding of national security information.

(2) establish written information security policies, procedures, and an effective information security education program.

(3) initiate and supervise measures or instructions necessary to ensure continual control of classified and sensitive information and materials.

(4) ensure that persons requiring access to classified information are properly cleared. The clearance status of each individual must be recorded and accessible for verification.

(5) review the effectiveness of the information security program in FCC bureaus and offices.

(6) ensure the prompt and complete reporting of security incidents, violations, and compromises, related to classified and sensitive information, as directed herein.

(7) ensure prompt reporting of credible derogatory information on assigned/attached personnel, to include recommendations for or against continued access.

(8) advise and assist officials on classification problems and the development of classification guidance.

(9) ensure that classification guides for classified plans, programs, and projects are properly prepared, distributed, and maintained.

(10) conduct a periodic review of classifications to ensure that classification decisions are proper.

(11) consistent with operational and statutory requirements, review all classified and sensitive documents in coordination with the FCC Records Management Officer. Continually reduce, by declassification, destruction, or retirement, unneeded classified and sensitive material.

(12) supervise or conduct security inspections and spot checks and notify the Managing Director regarding compliance with security regulations and directives.

(13) ensure that investigations and reporting of security violations is completed, including compromises or other threats to the safeguarding of classified and

sensitive information. Recommend corrective actions that should be taken concerning security violations.

(14) ensure proposed public releases on classified and sensitive programs be reviewed to preclude the release of classified information or other sensitive unclassified information covered under the Freedom of Information Act (FOIA).

(15) establish and maintain visit control procedures in cases in which visitors are authorized access to classified information.

(16) issue contingency plans for classified and sensitive information and material and, where necessary, for the safeguarding of classified and sensitive information and material.

D. Bureau and Office Chiefs. Chiefs of FCC Bureaus and Offices will

(1) ensure subordinate personnel who require access to classified information are properly cleared and are given access only to that information, including sensitive information, for which they have a need-to-know.

(2) ensure subordinate personnel are trained in, understand, and follow the requirements of this directive and Commission policy and procedures concerning the information security program.

(3) ensure personnel follow procedures necessary to allow the continuous safeguarding and control of classified and sensitive information.

David Robbins
Managing Director