FY 2021 Privacy & Data Protection Inspection (P&DP)

Report Number
21-INSP-10-01

March 29, 2024

OIG Highlights

What We Reviewed

The Office of Inspector General (OIG) conducted an inspection in accordance with 42 U.S.C. § 2000ee-2, which requires each agency to establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to the agency employees and the public. Such procedures shall be consistent with legal and regulatory guidance, including Office of Management and Budget regulations, the Privacy Act of 1974, and section 208 of the E-Government Act of 2002. 42 U.S.C. § 2000ee-2(b)(1). Our objective of this inspection was to determine whether the Federal Communications Commission (FCC) has implemented effective privacy and data protection policies and procedures in accordance with federal laws, regulations, and policies, with a focus on the FCC's implementation of the nine requirements identified in 42 U.S.C. § 2000ee-2 Privacy and Data Protection Policies and Procedures. The scope of this privacy and data protection inspection was from October 1, 2020, to September 30, 2021.

What We Found

Based on our inspection, the OIG concluded that the FCC has effectively implemented five of the nine privacy requirements in 42 U.S.C. § 2000ee-2. Four of the nine requirements had not been effectively implemented for the period covered by our review.

The FCC Office of the Chief Information Officer (OCIO) does not have any privacy-specific technologies in place for the use, collection, and disclosure of information in an identifiable form. The FCC is not in compliance with the agency's established privacy and data protection policies related to the use of automated technologies and continuous monitoring specific to privacy functions. The privacy staff was unable to support privacy impact assessments (PIAs) of proposed rules for the scope of the inspection. Lastly, we found two outdated policies related to privacy and data protection.

What We Recommended

We made seven recommendations for improvements related to the Commission's privacy and data protection policies and procedures.

1. Retain knowledgeable expertise in the FCC IT/privacy staff that will assist in implementing and sustaining the use of required privacy protections.
2. Implement a baseline of technologies that sustain and do not erode privacy protections relating to the use, collection, and disclosure of information.

3. Implement the Endpoint Detection and Response (EDR) tool that was previously acquired for privacy protection.
4. Identify and implement other technologies that will bring the FCC into full compliance with the requirement for continuous auditing of compliance with stated privacy policies and practices.
5. Document a formal process to perform PIAs for proposed rules, including details on the type of personally identifiable information collected and the number of people affected, in the FCC Privacy Act Manual, as a requirement.
6. Update the FCC Privacy Act Manual to include conducting PIAs for proposed rules.
7. Follow existing processes to annually review and update all privacy policies and directives. In particular, ensure that the FCC Directive 1113.1 – FCC Privacy Act Manual, and 1113.2 – Compliance with Privacy Laws and Guidance, are updated.

Table of Contents

Background

The FCC regulates interstate and international communications through cable, radio, television, satellite, and wire, and is the federal agency responsible for implementing and enforcing America's communications laws and regulations.

The FCC Privacy Program, headed by the Senior Agency Official for Privacy (SAOP), establishes the policies and assigns responsibilities for the FCC to carry out the requirements of the Privacy Act of 1974 and generally follow good privacy practices. Alongside the SAOP, the FCC Office of the Chief Information Officer (OCIO) shares responsibility for preserving and protecting personally identifiable information (PII) through data protection tools and technology resources and on-going coordination for compliance with privacy directives.

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that govern the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. Agencies are required to protect this information from any anticipated threats or hazards to their security or integrity, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual for whom the information is maintained.

The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act also provides individuals a way to seek access to and amendment of their records, and sets forth various agency record-keeping requirements. The information collected is considered a record under the Privacy Act if it is an item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, their education, financial transactions, medical history, and criminal or employment history and that contains a name or other identifier assigned to the individual.

Objective, Scope, And Methodology

The objective of the FY 2021 Privacy and Data Protection Inspection was to determine whether the FCC implemented effective privacy and data protection policies and procedures in accordance with applicable federal law, regulations, and policies and procedures. We focused on the nine requirements identified in 42 U.S.C. § 2000ee-2 Privacy and Data Protection Policies and Procedures. The scope of the privacy and data protection inspection covered the period from October 1, 2020, to September 30, 2021 (FY 2021).

During this inspection, the OIG audit team met with key personnel at the FCC. Additionally, the team reviewed documentation related to the FCC's privacy program, privacy related policies and procedures, lists of PII, privacy impact assessments, and technical controls related to data protection. We conducted this inspection in accordance with the Quality Standards for Inspection and Evaluation (Blue Book) adopted by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). Those standards require that we plan and perform the inspection to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our inspection objectives. We believe that the evidence obtained provides a reasonable basis for the findings and conclusions.

Appendix A includes additional details on the inspection, objectives, scope, and methodology.

Inspection Results

OIG inspected and tested the following nine requirements identified in 42 U.S.C. § 2000ee-2 Privacy and Data Protection Policies and Procedures to reach conclusions about the FCC's privacy program. Out of the nine requirements, we determined that the Commission was in compliance with five: requirements 3, 4, 6, 7, and 8. We identified items of non-compliance with requirements 1, 2, 5, and 9. See Table 1 below for OIG's conclusions on tests performed during the inspection.

Table 1 – Status of Requirements Testing

Requirement	Title 42 U.S.C. § 2000ee-2 Requirement Description	Demonstrated Compliance? Yes or No
1	Assuring that the use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form	No
2	Assuring that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program	No
3	Assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as defined in the Privacy Act of 1974	Yes
4	Evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the federal government	Yes
5	Conducting a PIA of proposed rules of the Agency on the privacy of information in an identifiable form, including the type of PII collected and the number of people affected	No
6	Preparing a report (i.e., annual FISMA Privacy Report) to Congress on an annual basis on activities of the Agency that affect privacy, including complaints of privacy violations, implementation of 5 U.S.C. § 552a, internal controls, and other relevant matters	Yes
7	Ensuring that the Agency protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction	Yes
8	Train and educate employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies	Yes
9	Ensuring compliance with the Agency's established privacy and data protection policies	No

Finding 1
FCC's Use of Technologies to Sustain Privacy and Data Protection Needs Improvement

42 U.S.C. § 2000ee-2 requires entities to assure that the use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form (requirement 1).

We reviewed the FCC's processes on how its information system supports privacy through the use of automated privacy controls. We determined that the FCC had not implemented technologies to ensure that privacy data protections relating to the use, collection, and disclosure of information are sustained. These privacy data protections should include activities related to cloud computing, wireless access, public key infrastructure, cryptography, mobile, and voice over IP devices. The FCC implemented Microsoft 365 capabilities that provide data protection for emails. However, the FCC has not implemented specific comprehensive protection technologies to sustain the use, collection, and disclosure of information in an identifiable form.

FCC OCIO personnel stated that they had not implemented the use of technologies specific to privacy protections due to higher priorities and new agency initiatives that have taken precedence, and a lack of expertise in this area. The FCC OCIO has acquired but not yet implemented other technology for privacy protections. They stated that they plan to submit a Business Requirement Document (budget request) for additional resources to implement required privacy protections.

By implementing technologies that protect privacy, the FCC can mitigate risks to PII, thereby limiting the impact of information system breaches and other privacy-related incidents.

Recommendations

The FCC OIG recommends that the FCC OCIO and SAOP:

1. Retain knowledgeable expertise in the FCC IT/Privacy staff that will assist in implementing and sustaining the usage of required privacy protections.
2. Implement a baseline of technologies that sustain and do not erode privacy protections relating to the use, collection, and disclosure of information.

Finding 2
The FCC's Use of Technologies for Continuous Auditing of Privacy Needs Improvement

42 U.S.C. § 2000ee-2 requires entities to assure that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program (requirement 2).

To determine if the FCC has met this requirement, we performed inquires and observations with relevant, key FCC personnel to gain an understanding about whether the FCC monitors and audits privacy controls and internal privacy policy.

We found that the FCC OCIO had not implement technologies that allow for continuous auditing

of compliance with stated privacy policies and practices governing the use, collection, and distribution of information in identifiable form. The FCC OCIO had not implemented the technologies specific to privacy protections because, as officials stated, they were handling priorities and new agency initiatives that took precedence. They also stated that they lacked expertise in this area.

During the scope of the inspection, the FCC OCIO had acquired, but not yet implemented, other technology for privacy protections. Officials stated that an endpoint detection and response (EDR) technology tool, specifically geared towards privacy, is being installed on Commission government furnished equipment laptops, but was not fully implemented. Privacy controls that allow for continuous auditing related to privacy processes and practices mitigate risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents. Also, privacy controls that monitor information use and sharing ensure that organizations use and share according to the authorized purposes identified in the Privacy Act or public notice, in a manner compatible with those purposes**.**

NIST 800-53, Rev. 4, (Control) AR-7 Privacy-Enhanced System Design and Development prescribes that organizations should design information systems to support privacy by automating privacy controls.

Recommendations

The FCC OIG recommends that the FCC OCIO:

3. Implement the EDR tool that was previously acquired for privacy protection.
4. Identify and implement other technologies that will bring the FCC into full compliance with the requirement for continuous auditing of compliance with stated privacy policies and practices.

Finding 3
The FCC's Privacy Impact Assessment (PIA) Process for Proposed Rules Needs Improvement

42 U.S.C. § 2000ee-2 requires entities to conduct a PIA of proposed rules of the Agency on the privacy of information in an identifiable form, including the type of PII collected and the number of people affected (requirement 5).

We requested evidence of any PIAs of proposed rules processed during FY 2021 and the privacy staff was unable to provide support of PIAs of proposed rules. The privacy staff explained their practice was to review proposed rules as a part of their work within the Office of General Counsel (OGC) but they did not follow a formal PIA process for each proposed rule.

M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, requires agencies to conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available.

The E-Government Act further requires agencies to conduct a PIA before:

- Developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or
- Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

The privacy team informed OIG that, while they worked within OGC and with other offices and bureaus to assess privacy implications, they did not follow a formal PIA process specific to proposed rules. Documenting a formal process for conducting PIAs of proposed rules ensures that Commission rules and orders inclusively and informatively account for the type of PII collected and the number of people affected.

Recommendations

The FCC OIG recommends that the FCC OCIO and SAOP:

5. Document a formal process to perform PIAs for proposed rules, including details on the type of personally identifiable information collected and the number of people affected, in the FCC Privacy Act Manual, as a requirement.
6. Update the FCC Privacy Act Manual to include conducting PIAs for proposed rules.

Finding 4
Ensure annual updates to the FCC's Privacy and Data Protections Policies and Directives

42 U.S.C. § 2000ee-2 requires entities to ensure compliance with the Agency's established privacy and data protection policies (requirement 9).

We inspected the FCC policies and directives to ensure compliance with privacy and data protection processes and validate periodic updates, including any updates to referenced policy documents.

The FCC privacy staff failed to follow their process to make annual updates to all privacy policies and directives. Our inspection noted that the FCC privacy staff had not updated the following directives during the inspection period and also by the end of our fieldwork on June 30, 2023:

- The FCC Directive 1113.1 – "FCC Privacy Act Manual" used to transmit the FCC Privacy Act Manual was last updated in March 2016.
- The FCC Directive 1113.2 – "Compliance with Privacy Laws and Guidance" for compliance with Privacy Laws and Guidance was last updated in April 2016.

The FCC Directive 1113.2 requires periodic updates to the Privacy Act Manual issued for compliance with Privacy Laws and Guidance. The FCC Cyber Security and Privacy Policy requires all mission and business processes relating to Cyber Security and Privacy policies and minimal use of PII in testing, training, and research be reviewed and revised annually.

OMB M-06-15 (replaced by OMB memorandum M-17-12) requires the Senior Official for Privacy to review agency policies and processes and take corrective action as appropriate to ensure adequate safeguards of PII.

The FCC management and SAOP failed to follow their process to update privacy policies and directives annually due to higher management priorities and new agency initiatives that took precedence. Failure to update the FCC policies and directives, when the federal guidance to which the FCC policies are referencing has been updated, increases the risk that the agency may not be in compliance with updated federal requirements. As an example, the directive on the FCC Privacy Act manual has not been updated since 2016, notwithstanding changes to federal requirements and guidance. Annual updates to privacy policies and directives ensure the FCC meets its statutory obligations to protect individual PII it collects, uses, maintains, and disseminates, and to safeguard and report on PII stored on its information systems.

Recommendation

The FCC OIG recommends that the FCC SAOP:

7. Follow existing processes to annually review and update all privacy policies and directives. In particular, ensure that the FCC Directives 1113.1 – The FCC Privacy Act Manual, and 1113.2 – Compliance with Privacy Laws and Guidance are updated.

APPENDIX A – Objective, Scope, and Methodology

Objective

The objective of the FY 2021 Privacy and Data Protection Inspection was to determine whether the FCC implemented effective privacy and data protection policies and procedures in accordance with applicable federal law, regulations, and policies and procedures, with a focus on the following nine requirements identified in 42 U.S. Code § 2000ee-2 Privacy and Data Protection Policies and Procedures.

Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including:

1. Assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form;

2. Assuring that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance, with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program;

3. Assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as defined in the Privacy Act of 1974 [5 U.S.C. 552a];

4. Evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the federal government;

5. Conducting a privacy impact assessment of proposed rules of the Department on the privacy of information in an identifiable form, including the type of personally identifiable information collected and the number of people affected;

6. Preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of Section 552a of Title 5, 11 internal controls, and other relevant matters;

7. Ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction;

8. Training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies; and

9. Ensuring compliance with the Department's established privacy and data protection policies.

Scope

The privacy and data protection inspection included a review of whether the FCC implemented an effective data protection and privacy program from October 1, 2020, to September 30, 2021.

To accomplish our inspection objectives, we performed inspection procedures, as deemed appropriate, including the following:

- Reviewed federal laws, regulations, and guidance applicable to the Privacy and Data Protection Inspection;
- Requested and reviewed policies and procedures developed and implemented for the Privacy and Data Protection Inspection;
- Requested information needed to develop the inspection plan for the nine requirements identified 42 U.S.C. § 2000ee-2 Privacy and Data Protection Policies and Procedures;
- Assessed overall sufficiency and appropriateness of the evidence obtained during inspection;
- Interviewed the Acting CIO and SAOP to obtain an understanding of the FCC's privacy and data protection related program;
- Conducted meetings with relevant key FCC IT personnel and inspected relevant documentation to understand how the FCC's information system design supports privacy by automating privacy controls and provides assurance that the use of technologies sustains, and does not erode privacy protections relating to the use, collection, and disclosure of PII;
- Inspected the FCC's inventory listing that captures and stores PII and documentation on the FCC processes for reviewing the FCC's PII holdings;
- Inspected the FCC website privacy related requirements (including third party websites that host PII) and their compliance with the FCC's policies and procedures as well as regulatory requirements;
- Inspected a representative sample of completed PIAs to ensure compliance with the FCC and regulatory requirements;
- Inspected evidence to test accurate accounting of disclosures of records is maintained in a representative sample system of record; and
- Inspected the inventory listing of the FCC's basic privacy training conducted during the inspection period.

APPENDIX B

Office of the Managing Director
MEMORANDUM

DATE: March 15, 2024

TO: Sharon Diskin – Acting Inspector General

FROM: Mark Stephens, Managing Director
Elliot S. Tarloff, Senior Agency Official for Privacy

SUBJECT: Management's Response to the Fiscal Year 2021 Privacy and Data Protection Inspection (21-INSP-10-01)

Thank you for the opportunity to review and comment on the draft report, *FY 2021 Privacy and Data Protection Inspection*, Number 21-INSP-10-01.

We appreciate the efforts of the FCC's Office of the Inspector General (OIG) to work with the Federal Communications Commission (FCC or Commission) throughout the inspection. The report is the result of the commitment and professionalism demonstrated by the OIG, the Office of the Managing Director (OMD) (specifically the Office of the Chief Information Officer (OCIO)), and the Office of the General Counsel (OGC) (specifically the Privacy Program). During the course of the inspection, Commission staff and contractors worked closely with OIG staff to provide the requested information in a timely manner, to facilitate the inspection process.

We are pleased to concur with your finding that, during the inspection period, the FCC had effectively implemented five of the nine privacy requirements codified in 42 U.S.C. § 2000ee-2. We also concur with your finding that, during the inspection period, the FCC had not effectively implemented four of those nine requirements. We similarly concur with—and appreciate—your seven recommendations to assist the FCC's full implementation of the four open requirements.

The FCC is committed to continually strengthening its cybersecurity and privacy programs. We look forward to leveraging your findings and recommendations to drive continued progress in our efforts. As you know, since the period covered by the inspection, the FCC has gone through changes in leadership in both OCIO and the Privacy Program. As these two teams continue to evolve and collaborate, we have already begun working to resolve your findings and to implement your recommendations.

Indeed, with respect to the findings and recommendations directed specifically to the FCC Privacy Program, the Privacy team has made meaningful progress. Since concurring with the relevant OIG findings and Recommendations, the Privacy Team has:

- Completed an initial-draft process and checklist to perform privacy impact assessments for proposed rules and other Bureau- and Commission-level items;
- Started the process of editing the Privacy Act Manual—to be restyled the Privacy Program Manual—which will include the process and checklist to perform privacy impact assessments for proposed rules; and
- Started the process of editing Directive 113.1, Privacy Act Manual—to be restyled the Privacy Program Manual—and completed the recission of Directive 1113.2, Compliance with Privacy Laws and Guidance, which has been fully incorporated into, and replaced by Directive 1479.7.

Please also note that the Privacy Program identified completing, in FY 24, the process of updating and restyling the Privacy Act Manual as a Strategic Objective in the FCC's FY 23 Privacy Program Plan, which we submitted to the Office of Management and Budget and Department of Homeland Security in connection with the required annual SAOP metrics.

We look forward to updating you as we continue to make progress on these recommendations and findings.

*****

In partnership with the Bureaus and Offices across the Commission, OCIO and the Privacy Program remain committed to strengthening the FCC's privacy and data protection policies and procedures. We look forward to working in this coming fiscal year to resolve the inspection report's findings while continuing to enhance the cybersecurity and privacy posture of the Commission.

Respectfully submitted,

MARK STEPHENS Digitally signed by MARK STEPHENS Date: 2023.12.21 16:26:44 -05'00'

Mark Stephens
Managing Director
Office of Managing Director

ELLIOT TARLOFF Digitally signed by ELLIOT TARLOFF Date: 2024.03.15 08:40:03 -04'00'

Elliot Sheppard Tarloff
Senior Agency Official for Privacy
Office of General Counsel

APPENDIX C
Glossary of Acronyms and Abbreviations

Acronym	Definition
CIGIE	Council of Inspectors General on Integrity and Efficiency
Commission	Federal Communications Commission
EDR	Endpoint detection and response tool
FISMA	Federal Information Systems Modernization Act
GFE	Government Furnished Equipment
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OMD	Office of the Managing Director
PBC	Provided by client
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SAOP	Senior Agency Official for Privacy
U.S.C.	U.S. Code

HELP FIGHT

FRAUD. WASTE. ABUSE.

Toll free at 1-888-863-2244 or call 1-202-418-0473

https://www.fcc.gov/general/office-inspector-general-hotline