SPECTRUM IT MODERNIZATION

NTIA Should Fully Incorporate Cybersecurity and Interoperability Practices

Report to Congressional Committees

May 2025
GAO-25-107509
United States Government Accountability Office

Accessible Version

GAO Highlights

For more information, contact Vijay A. D'Souza at dsouzav@gao.gov.
Highlights of GAO-25-107509, a report to congressional committees

May 2025

SPECTRUM IT MODERNIZATION
NTIA Should Fully Incorporate Cybersecurity and Interoperability Practices

Why GAO Did This Study

Use of the radio frequency spectrum is vital to a wide variety of commercial and government activities. NTIA currently manages federal spectrum by relying on IT systems that are out of date and present usability challenges. In 2021, Congress required NTIA to create a plan for modernizing its spectrum IT systems.

As part of the same legislation, Congress required GAO to biennially review NTIA's efforts to modernize its spectrum IT systems. This review examines the extent to which NTIA's plans to modernize its spectrum IT infrastructure incorporated leading practices for (1) cybersecurity and (2) interoperability.

To do so, GAO compared NTIA modernization planning against selected practices for risk management, systems security, and cloud security. GAO compared NTIA information on interagency collaboration and data standard development against leading practices identified in prior GAO work to evaluate support for organizational interoperability. GAO also interviewed relevant NTIA officials.

What GAO Recommends

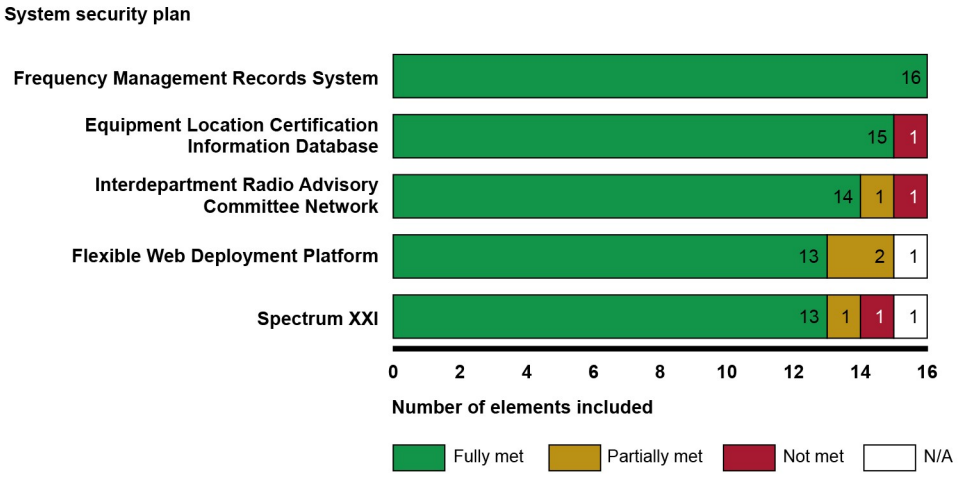
GAO is making five recommendations to NTIA to implement leading practices on completing an organization-wide risk assessment, developing a risk strategy, maintaining current system security plans, defining cloud access management procedures, and developing a data governance plan. NTIA concurred with the recommendations and stated it will develop an action plan to implement them.

What GAO Found

The National Telecommunications and Information Administration (NTIA) is responsible for managing federal use of radio frequency spectrum. It is now more than three years into a planned modernization of its spectrum IT systems. In December 2024, NTIA awarded two contracts totaling $110 million to support the modernization. The first task order planned under these contracts is expected to include a program roadmap and schedule. Accordingly, NTIA will continue to rely on existing legacy IT systems for the near future.

In planning the modernization, NTIA implemented many leading cybersecurity practices but partially implemented or did not address other such practices. For example, it took steps to categorize and manage risks to its legacy spectrum IT systems. In addition, NTIA has defined key requirements for its cloud service provider. However, it has not fully developed a risk management strategy and has not completed an organization-wide risk assessment. Further, while it has developed system security plans that address most required elements (see fig.), these plans were not always current. Also, in its cloud access management policies, NTIA did not fully define user privilege levels for its systems. Fully implementing leading practices can enable NTIA to identify, track, mitigate, and reduce cybersecurity risks during the remainder of its modernization effort.

Assessment of NTIA Spectrum IT System Security Plan Elements



Source: GAO review of National Telecommunications and Information Administration (NTIA) documentation. | GAO-25-107509

Accessible Data for Assessment of NTIA Spectrum IT System Security Plan Elements

System security plan	Fully met	Partially met	Not met	N/A
Frequency management records system	16	0	0	0
Equipment location certification information database	15	0	1	0
Interdepartment radio advisory commit-tee network	14	1	1	0
Flexible web deployment platform	13	2	0	1
Spectrum XXI	13	1	1	1

Source: GAO review of National Telecommunications and Information Administration (NTIA) documentation. I GAO-25-107509

Regarding interoperability planning, NTIA met most interagency collaboration and data standards leading practices. In planning its modernization, NTIA incorporated all of GAO's eight leading practices for collaboration with its partner agencies, such as defining common outcomes and including relevant partner agency participants. NTIA also fully implemented three of five leading practices for data governance. For example, its ongoing replacement of its data standard, an important step in its modernization effort, involved stakeholders in key decisions. However, it has not developed a data governance plan that details how conflicts resulting from use of the new standard will be resolved and defines roles and responsibilities for the remaining implementation and maintenance of the standard. Until NTIA completes such a plan, NTIA and its partners may face issues in exchanging and processing spectrum IT data.

Contents

Abbreviations

- CONOPS concept of operations
- DCFS Data Capture and Forwarding System
- DOD Department of Defense
- EL-CID Equipment Location Certification Information Database Online
- FAS Frequency Assignment Subcommittee
- FCC Federal Communications Commission
- FedRAMP Federal Risk and Authorization Management Program
- FMRS Frequency Management and Reporting System
- FY fiscal year
- FY21 NDAA William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021
- GMF Government Master File
- ICAM identity, credential, and access management
- IRAC Interdepartment Radio Advisory Committee
- IRACNet Interdepartment Radio Advisory Committee Network
- IT information technology
- NIST National Institute of Standards and Technology
- NTIA National Telecommunications and Information
- Administration
- OMB Office of Management and Budget
- RMF risk management framework
- SNSS Spectrum National Security Systems
- SSP system security plan
- SXXI Spectrum XXI
- XML eXtensible Markup Language

May 22, 2025

Congressional Committees

The radio frequency spectrum is a scarce, natural resource used to support a wide variety of vital commercial and government activities.[1] For example, commercial entities use spectrum to provide wireless high-speed internet and broadcast television, while federal agencies use it for missions ranging from national defense to air traffic control.[2] Spectrum needs are expected to increase due to 5G telecommunications and other new technologies.

As spectrum use increases, U.S. frequency management is transitioning from primarily static methods to a more dynamic approach, including time- and location-based spectrum sharing techniques. We have previously reported on the importance of efficiently managing spectrum to meet this increasing demand.[3] Effectively managing spectrum resources is integral to a functioning federal government.

The Department of Commerce's National Telecommunications and Information Administration (NTIA) manages spectrum use for federal users.[4] For example, NTIA assigns spectrum to federal agencies, providing them with authorization to operate in defined frequency bands. To manage spectrum, NTIA relies on a combination of multiple custom software applications, databases, engineering tools, and other spectrum-related information technology systems (hereafter, IT or IT systems). NTIA provides access to these IT systems to agencies that use spectrum. Additionally, some of these agencies have their own internal, custom IT to help manage spectrum use.[5]

However, we have previously reported that NTIA's IT systems are out of date and, according to NTIA officials, present various challenges for the agency that hinder its ability to efficiently manage spectrum.[6] For example, the systems require that NTIA use manual processes for managing tens of thousands of requests for frequency assignments from federal agencies each year. We have previously found that federal agencies with

[1]The radio frequency spectrum is a part of the natural spectrum of electromagnetic radiation. Frequencies, which are grouped into bands, are properties of electromagnetic waves that describe how many wave patterns or cycles pass by in a period of time.

[2]For the purposes of this report, the term "agency" refers to either a federal agency or an agency's component, as consistent with the list of "covered agencies" for section 9203 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA). See Pub. L. No. 116-283, § 9203(e)(1), 134 Stat. 3388, 4797 (2021).

[3]See, for example, GAO, *Spectrum Management: NTIA Should Improve Spectrum Reallocation Planning and Assess Its Workforce*, GAO-22-104537 (Washington, D.C.: Jan. 27, 2022).

[4]Within the United States, spectrum is jointly managed by NTIA and the Federal Communications Commission (FCC) —an independent agency within the executive branch. NTIA manages spectrum for federal government users and advises the President on telecommunications issues, while FCC manages spectrum use for nonfederal users, including commercial, individual, and state and local government users.

[5]For additional information on the IT that NTIA and other agencies use and operate, see GAO, *Spectrum Management: Information Technologies for Managing Federal Use*, GAO-22-105221 (Washington, D.C.: Feb. 17, 2022).

[6]GAO-22-105221.

outdated legacy IT systems, such as NTIA's systems, face a variety of risks in using the technology and could improve their modernization efforts.[7]

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA) required NTIA to develop and submit to Congress a plan to modernize its IT to more efficiently manage spectrum.[8] It also required other covered agencies to develop and submit plans to modernize their own spectrum IT systems in a manner that maintains interoperability with NTIA's modernized systems. NTIA subsequently designated the agencies that are part of the Interdepartment Radio Advisory Committee (IRAC)—a committee responsible for advising NTIA on spectrum issues—as the covered agencies required to issue modernization plans.[9]

The FY21 NDAA includes a provision for GAO to biennially review NTIA's and the covered agencies' IT modernization. Previously, GAO published a report examining the extent to which NTIA's modernization project planning incorporated leading practices for effective IT modernization and project management.[10] Our current review focuses on NTIA's plans to modernize its spectrum IT infrastructure with respect to cybersecurity and interoperability. Specifically, our objectives were to (1) determine the extent to which NTIA plans to modernize its spectrum IT infrastructure incorporated leading practices for cybersecurity and (2) determine the extent to which NTIA plans to modernize its spectrum IT infrastructure incorporated leading practices for interoperability.

To address our first objective, we

- compared NTIA plans and practices[11] against guidance from the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) to determine whether NTIA took steps to improve its posture for managing security and privacy risks;[12]
- compared NTIA system security plans (SSP) for its primary spectrum IT systems against NIST guidance to determine whether NTIA documented key information needed to evaluate the security of its systems;[13] and

[7]See, for example, GAO, *Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements*, GAO-23-104719 (Washington, D.C.: Jan. 12, 2023).

[8]The FY21 NDAA defines a covered agency as the Department of Defense (DOD) as well as any federal entity that the head of NTIA determines is appropriate. Pub. L. No. 116-283, § 9203(e)(1), 134 Stat. 4797.

[9]NTIA chairs IRAC, which includes a variety of subcommittees that have specialized functions, such as assisting NTIA in assigning frequencies. The IRAC consists of NTIA and the following entities: Departments of Agriculture, Commerce, Defense (including the Air Force, Army, and Navy), Energy, Homeland Security, Interior, Justice, State, Transportation, Treasury, and Veterans Affairs, as well as the Federal Aviation Administration, National Aeronautics and Space Administration, National Science Foundation, U.S. Agency for Global Media, U.S. Coast Guard, and U.S. Postal Service. NTIA also designated the Federal Communications Commission, a liaison to the IRAC, as a covered agency.

[10]GAO, *Spectrum IT Modernization: Incorporating Leading Practices Could Improve Planning Effort*, GAO-24-106634 (Washington, D.C.: Mar. 19, 2024).

[11]In selected instances where NTIA had not made sufficient progress to perform a complete analysis, we compared documentation on NTIA legacy systems against the leading practices.

[12]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2 (Gaithersburg, MD: December 2018).

[13]National Institute of Standards and Technology, *Guide for Developing Security Plans for Federal Information Systems*, Special Publication 800-18, Revision 1 (Gaithersburg, MD: February 2006).

- compared NTIA actions to improve the cloud security of its spectrum IT systems against key cloud security practices to determine the extent to which the agency incorporated these key practices.[14]

To address our second objective, we evaluated NTIA information to inform whether its modernization planning facilitated greater interoperability between its systems and those of its users. To determine this, we reviewed information in NTIA plans, policies, and other modernization-related documentation on interagency collaboration and data standards. We considered adherence to these leading practices as a reasonable representation of the status of organizational interoperability planning, since full operational interoperability depends on shared governance structures facilitated by cross-agency coordination.

In particular, we compared actions taken by NTIA to coordinate with federal agency partners in planning its modernization against leading practices for interagency collaboration developed in prior GAO work.[15] We also compared NTIA plans for developing and implementing an interoperable data standard against relevant key practices identified in prior GAO work.[16]

We supplemented our analyses with interviews of relevant officials within NTIA's Office of Spectrum Management and the IT Division within NTIA's Office of Policy Coordination and Management. Further details on our objectives, scope, and methodology are included in appendix I.

We conducted this performance audit from April 2024 to May 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

NTIA manages federal use of spectrum, a limited natural resource. The agency is responsible for promoting the best possible and most efficient use of spectrum resources across the federal government, subject to and consistent with the needs and missions of federal agencies. NTIA follows a multistep process to assign spectrum to federal agencies.[17] This process is intended to prevent harmful interference between different users, such as if two agencies request spectrum, are assigned adjacent frequencies, and attempt to send transmissions at the same time in the same area in a manner that would result in disruptions. NTIA also certifies the spectrum-dependent equipment (i.e., communication devices that rely on spectrum to transmit a

[14]See GAO, *Cloud Security: Selected Agencies Need to Fully Implement Key Practices*, GAO-23-105482 (Washington, D.C.: May 18, 2023). The six cloud security key practices were selected by GAO based on a review of federal policies and guidance and with input from public and private sector experts.

[15]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 24, 2023).

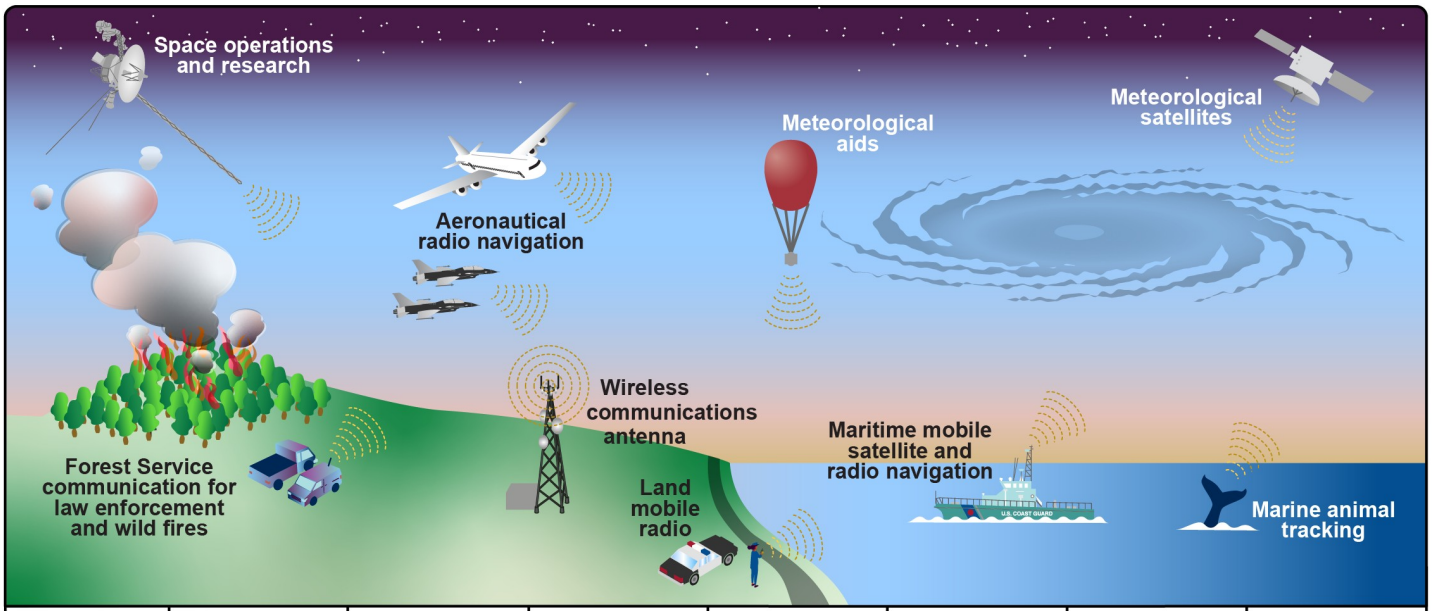
[16]GAO, *DATA Act: OMB Needs to Formalize Data Governance for Reporting Federal Spending*, GAO-19-284 (Washington, D.C.: Mar. 22, 2019); and *DATA Act: OMB and Treasury Have Issued Additional Guidance and Have Improved Pilot Design but Implementation Challenges Remain*, GAO-17-156 (Washington, D.C.: Dec. 8, 2016).

[17]In this process, agencies make an initial request for spectrum; NTIA electronically processes the request and checks for errors, such as formatting mistakes in the request; and members of the IRAC Frequency Assignment Subcommittee review the requests and resolve disputes between agencies. Prior to submitting a frequency request, agencies may use various NTIA IT systems to check for potential interference.

signal) that federal agencies acquire. This certification is designed to ensure that the equipment conforms to federal spectrum standards and can operate in available spectrum.

After receiving a spectrum allocation, federal agencies use their assigned spectrum for a broad range of activities. Figure 1 shows the range of activities across the federal government for which spectrum allocations are used.

Figure 1: Examples of Federal Uses of Spectrum



Frequency ranges	30 kHz – 300 kHz	300 kHz – 3 MHz	3 MHz – 30 MHz	30 MHz – 300 MHz	300 MHz – 3 GHz	3 GHz – 30 GHz	30 GHz – 300 GHz
Examples of federal spectrum use	Maritime mobile	Mobile communications	Radar	Mobile communications	Meteorological satellite	Space research	Earth-to-space mobile communications

Sources: GAO illustrations and analysis of National Telecommunications and Information Administration information. | GAO-25-107509

To fulfill its responsibilities as spectrum manager, NTIA relies on a combination of custom software applications, databases, engineering tools, and other spectrum-related IT legacy systems. NTIA provides access to these systems to the other federal agencies that use spectrum. Table 1 lists the name and a brief description of each of NTIA's primary spectrum IT systems.

Table 1: Description of National Telecommunications and Information Administration (NTIA) Spectrum IT Management Systems

System name	System description
Spectrum XXI (SXXI)	Supports managing frequency assignments and authorizations and is used to submit frequency proposals to NTIA. This system is used by nearly all covered agencies to request frequency assignments from NTIA. The Department of Defense (DOD) is the owner of SXXI; however, NTIA operates a separate implementation of it and provides access to this system for other agencies through a government use agreement with DOD.
Frequency Management and Reporting System (FMRS)	Supports managing frequency assignments and authorizations. It is used to receive and process frequency proposals at NTIA on the classified network, resulting in updates to the Government Master File, NTIA's record of all federal frequency assignments.
Interdepartment Radio Advisory Committee Network (IRACNet)	Used by the Interdepartment Radio Advisory Committee (IRAC) and its subcommittees. IRAC's responsibilities include assisting the Assistant Secretary of Commerce for Communications and Information—the Administrator of NTIA—with regard to spectrum; including assigning frequencies to the U.S. Government Radio Station; and developing policies as they relate to spectrum. IRAC uses IRACNet to collaborate, facilitate IRAC meetings, and manage IRAC data. NTIA named the agencies that are members of IRAC as covered agencies as part of its authority under the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021).
Data Capture and Forwarding System (DCFS)	Supports the managing of frequency assignments and authorizations. It is used to receive and process frequency proposals at NTIA on its unclassified network. Information on frequency ranges is transferred from DCFS to FMRS for use regarding approved frequency assignment proposals.
Equipment Location Certification Information Database (EL-CID)	Electronically processes agency requests to NTIA to certify agencies' spectrum-dependent equipment. It is used to author, submit, receive, and process spectrum certification requests.
FreqCoord	Supports managing frequency assignments and authorizations. It is used to author, submit, and approve frequency proposals in selected frequency bands.
Spectrum Transition Tool	Supports the management of frequency reallocations and transitions. It is used to facilitate federal planning, tracking, and reporting of radio frequency transition activities, including spectrum sharing arrangements.

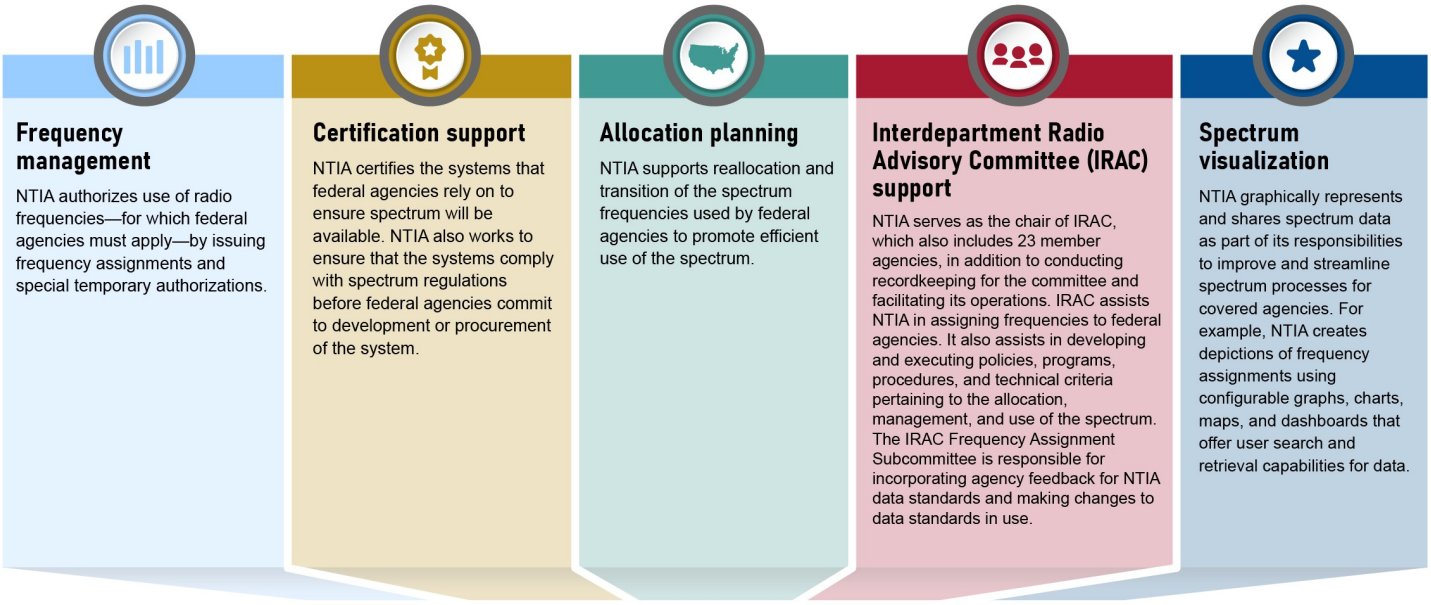
Source: GAO summary of NTIA documentation. | GAO-25-107509

NTIA Identified Mission Needs to Inform Its Spectrum IT Modernization

The FY21 NDAA required NTIA to modernize its spectrum IT infrastructure, including by taking steps to enhance cybersecurity and improve interoperability.[18] NTIA identified five primary needs for this modernization to enable it to accomplish its mission, including frequency management, allocation planning, and spectrum visualization. Figure 2 describes these mission needs.

[18]Pub. L. No. 116-283, § 9203(a)(1), (a)(6), b(2)(D), 134 Stat. 3388, 4793-94 (2021).

Figure 2: National Telecommunications and Information Administration (NTIA) Spectrum IT Mission Needs



Sources: GAO summary of NTIA documentation; endstem/stock.adobe.com (USA icon); Icons-Studio/stock.adobe.com (icons). | GAO-25-107509

NTIA considers its modernization effort as essential in filling capability gaps that have prevented it from fully meeting these mission needs. Further, according to NTIA officials, the modernization effort is a foundational part of future elements of NTIA operations, including the enhancement of spectrum sharing. To increase spectrum efficiency, federal agencies, including NTIA, plan to employ innovative spectrum management technologies and techniques.

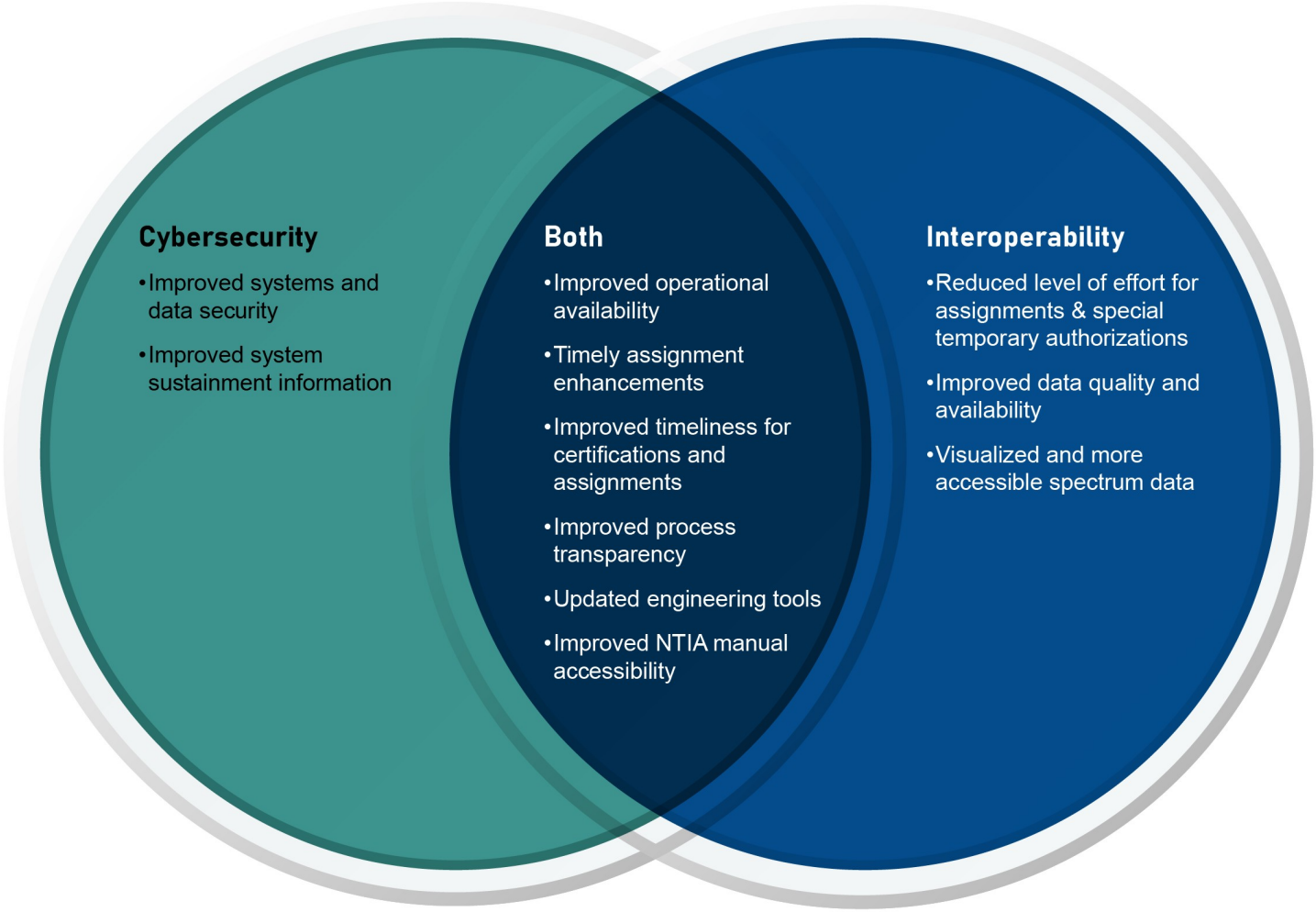
NTIA subsequently developed a more detailed mission needs statement for its modernization. In addition to the mission needs shown previously in figure 2, this statement describes specific goals, approaches, and capability gaps which the modernization is intended to fill to more fully meet mission needs.

As part of its mission needs documentation, NTIA established five goals for the modernization of its spectrum IT, two of which are directly related to improving the cybersecurity and interoperability of spectrum IT systems. Specifically, NTIA goals include

- strengthening the security of NTIA spectrum IT systems to ensure their continued availability for essential federal missions, and to protect spectrum data from unauthorized release and improper modification; and
- improving the accessibility, interoperability, and comprehensiveness of spectrum data.

These goals are directly reflected in the types of enhancements planned thus far as part of the modernization. Figure 3 categorizes some of the anticipated enhancements related to cybersecurity, interoperability, or both.

Figure 3: National Telecommunications and Information Administration (NTIA) Spectrum IT Modernization Anticipated Improvements



Sources: GAO analysis of NTIA documentation and circle illustrations. | GAO-25-107509

NTIA Has Taken Steps to Modernize Its Spectrum IT Systems

NTIA plans to obligate funding over a nine-year period (comprising fiscal years 2022 through 2030) to support its spectrum IT modernization project.[19] During the life cycle of the modernization, NTIA plans to keep its legacy spectrum IT systems in operation and retire these systems as their functionality is replaced.

In March 2024, NTIA received approval from the Commerce IT Review Board and the Acquisition Review Board to contract for the modernization. In December of that year, NTIA awarded two contracts with a total planned value of $110 million. According to contract documentation, the first task orders to be developed under

[19]In its fiscal year 2022 budget request, NTIA estimated that the spectrum IT modernization would cost $109 million. However, according to NTIA officials, this was a rough order of magnitude estimate, not a detailed cost estimate.

these contracts will include the development of a program roadmap and schedule. As of March 2025, it had yet to issue the task orders under these contracts.

NTIA has taken other steps to prepare for its modernization. Specifically:

- In September 2021, NTIA released a high-level statement of intent for the modernization.[20] This statement of intent highlighted the need to support current and future spectrum demands by improving the security, including cybersecurity, and interoperability of different spectrum IT legacy systems. According to officials, NTIA is still in the process of developing a more detailed overarching modernization plan and finalizing a time frame for its completion.
- NTIA established high-level acquisition milestone dates for modernizing the legacy spectrum IT systems that it manages, such as milestones for approval to initiate the work—March 2023—and to commence detailed planning—September 2024.[21] It has also begun to document in greater detail the work necessary to modernize and eventually retire the legacy systems.
- NTIA migrated all unclassified instances of its spectrum systems to the cloud as of September 2024 and plans to complete its classified migration by 2026.[22] According to NTIA officials, migrating its existing systems into the cloud first will provide a foundation for NTIA to scale its modernization reliably and securely.

GAO Previously Reported on NTIA's Modernization of Its Spectrum IT Systems

In February 2022, we reported that NTIA's goals for its IT modernization included addressing limitations in existing legacy systems and facilitating the potential for greater spectrum sharing.[23] Officials from covered agencies also suggested that enhanced cybersecurity and more precise data standards could improve spectrum management as part of the modernization. We did not make any recommendations in this report.

In March 2024, we reported that NTIA's spectrum IT modernization efforts did not align with leading practices for effective IT modernization and project management.[24] Specifically, we found that NTIA's planning efforts did not align with leading practices for developing a cost estimate, developing a schedule to complete the project, regularly communicating with stakeholders, and developing performance measures. Additionally, the extent to which NTIA's specific modernization plans would address the agency's stated improvement opportunities remained unclear. As a result, we made four recommendations to NTIA related to its modernization efforts, including to finalize its stakeholder management plan and to establish performance measures that link to established goals. NTIA concurred with our four recommendations but as of May 2025 has not yet implemented them.

[20]National Telecommunications and Information Administration, *Plan to Modernize and Automate the Infrastructure of NTIA Related to Managing Federal Spectrum Use* (Washington, D.C.: September 2021).

[21]In its role as system owner, DOD is developing a new version of the Spectrum XXI system and plans to review and validate capability requirements for the system. According to DOD officials, this modernized version of the system will meet NTIA requirements, pending further testing and a determination of deployment time frames.

[22]Systems with only unclassified instances include SXXI, FreqCoord, and the Spectrum Transition Tool. FMRS has only a classified instance. EL-CID, IRACNet, and DCFS have both classified and unclassified instances.

[23]GAO-22-105221.

[24]GAO-24-106634.

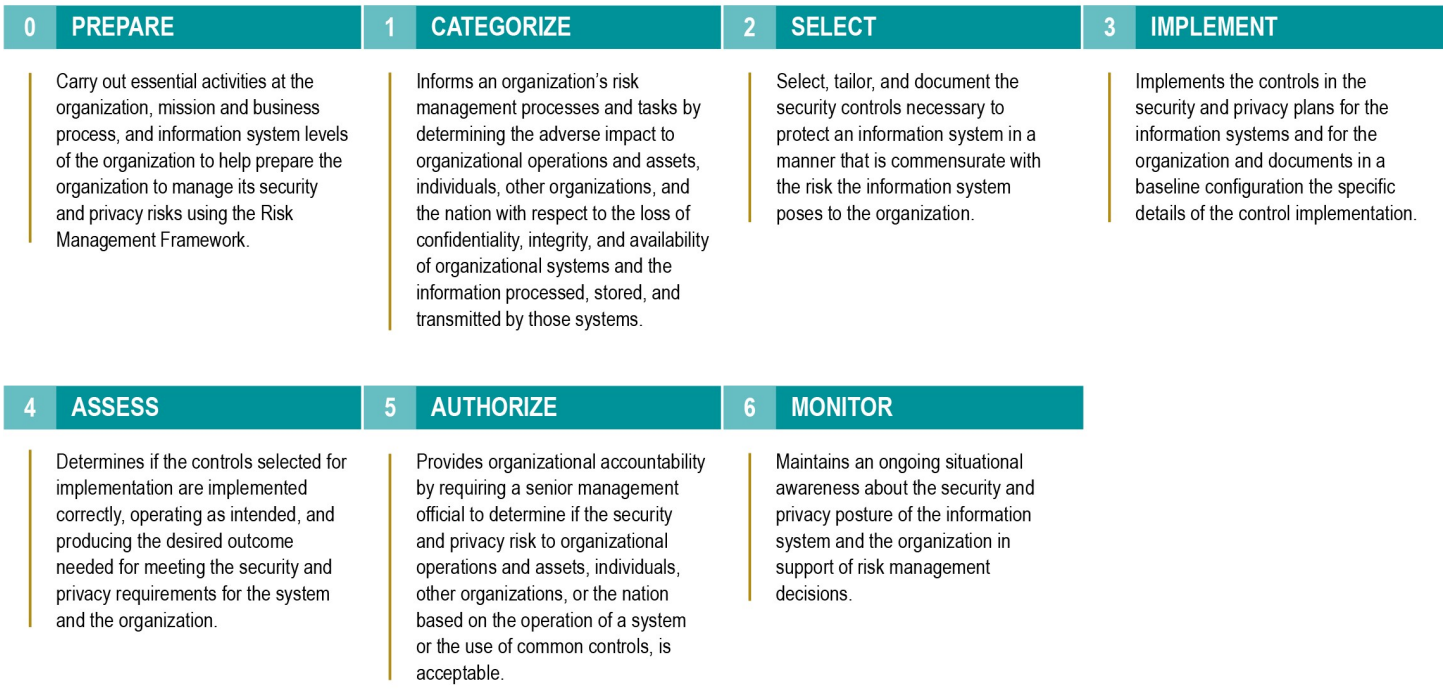
NTIA Did Not Fully Incorporate Selected Cybersecurity Practices for Its Spectrum IT Systems

NTIA implemented many cybersecurity practices for its spectrum IT systems. The agency partially met practices on developing a risk management strategy, identifying versions and changes made to system security plans, and documenting cloud access management policies and procedures. In addition, the agency did not meet practices on developing an organization-wide risk assessment or on conducting an annual review of some of its systems' security plans.

NTIA Did Not Fully Document Its Organization-Wide Risk Management Practices

Federal guidance from the Office of Management and Budget (OMB) requires that agencies develop a risk management process in accordance with NIST's risk management framework.[25] Specifically, the NIST framework identifies seven cybersecurity-related steps that agencies should perform to implement security and privacy requirements and controls, which are further broken down into associated tasks. The first two of these seven steps, on the preparation and categorization of cybersecurity risks, are critical for the planning of cybersecurity practices. Figure 4 shows the seven NIST risk management framework steps.

Figure 4: Steps of National Institute of Standards and Technology's (NIST) Risk Management Framework



Source: GAO analysis of NIST data. | GAO-25-107509

[25]Office of Management and Budget, Circular No. A-130, *Managing Information as a Strategic Resource*, (Washington, D.C.: July 28, 2016).

The purpose of the *prepare* step is to carry out activities at the organization and system level to enable the organization to manage its cybersecurity risks using the risk management framework. The *prepare* step includes five required organization-level tasks. Out of these five tasks, NTIA fully met three, partially met one, and did not meet one. Table 2 shows the extent to which each organization-level *prepare* task is covered in NTIA guidance.

Table 2: Assessment of National Telecommunications and Information Administration (NTIA) Spectrum IT Implementation of Required NIST RMF Organization-Level Prepare Step Tasks

Task	Assessment	Description of assessment
Risk Management Roles: Individuals are identified and assigned key roles for executing the Risk Management Framework	fully met criteria	NTIA policy assigns individual roles and responsibilities for cybersecurity and risk management. For example, NTIA assigned responsibility for providing technical support on system functionality and implementation of security safeguards to NTIA's authorizing official designated representative.
Risk Management Strategy: A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established	partially met criteria	NTIA officials stated that the agency follows the Department of Commerce Risk Management Strategy. Therefore, NTIA has not developed its own risk management strategy. However, the Department of Commerce Risk Management Strategy, due to its scope, does not contain certain information required at an organization level. Among other things, the strategy does not include an expression of organizational risk tolerance, and acceptable risk assessment methodologies and risk response strategies.
Risk Assessment—Organization: An organization-wide risk assessment is completed, or an existing risk assessment is updated	did not meet the criteria	NTIA did not conduct an organization-wide risk assessment that included aggregated information from system level risk assessment results and risk considerations relevant at the organization level. According to NTIA officials, NTIA does not conduct organization-wide risk assessments, and instead focuses on system-level risk assessments. NIST guidance recommends that an assessment be conducted at both organization-wide and system-wide levels.
Common Control Identification: Common controls that are available for inheritance by organizational systems are identified, documented, and published	fully met criteria	The Department of Commerce maintains a common controls database that identifies, documents, and publishes controls based on NIST guidance for establishing security and privacy controls. NTIA maintains a system that shows controls available for inheritance from the Commerce system, where users can manage, tailor, and implement inherited controls.
Continuous Monitoring Strategy—Organization: An organization-wide strategy for monitoring control effectiveness is developed and implemented	fully met criteria	The NTIA continuous monitoring strategy policy establishes the goals, objectives, and procedures for continuous monitoring activities and establishes NTIA's policy for monitoring security controls. Examples of continuous monitoring activities addressed in the plan include performing automated vulnerability and secure configuration scans using vulnerability management software every 72 hours and conducting a security impact analysis for all proposed changes to information systems.

Legend:
NIST = National Institute of Standards and Technology
RMF = Risk Management Framework
● = The agency fully met the criteria.
◐ = The agency partially met criteria.
○ = The agency did not meet the criteria.

Source: GAO analysis of NTIA documentation. | GAO-25-107509

Specifically:

- NTIA uses a strategy inherited from the Department of Commerce to conduct risk management activities. However, it did not fully develop an NTIA-specific risk management strategy that includes information such as preferred organizational risk tolerance and NTIA risk response strategies. NTIA officials stated that the agency does not need to complete an organization-level risk management strategy because it relies on the Department of Commerce strategy. However, Commerce's risk management strategy also does not include considerations suggested by NIST, such as an expression of organizational risk tolerance, acceptable risk assessment methodologies, and risk response strategies.
- NTIA has not performed a risk assessment focusing on organization-level risks. NTIA officials stated that the agency's focus is on conducting system-level risk assessments for each spectrum IT system, based on requirements in NTIA's risk management policy. However, NIST guidance states that a risk assessment should also be completed at an organization-wide level to centrally incorporate information from a series of system-level risk assessment results. According to the guidance, this assists agencies in determining, among other things, whether higher-impact systems are segregated from lower-impact systems.

Developing and documenting a comprehensive, organization-level risk management strategy and a corresponding risk assessment would better position NTIA to perform activities needed to support its cybersecurity risk responses, such as identifying relevant threats, vulnerabilities, and the impact that may result from exploitation of these vulnerabilities. Until it does so, NTIA is less able to identify and track progress in mitigating the cyber risks that are most impactful to the agency.

In addition, NTIA has taken action to implement several other optional *prepare* tasks recommended in NIST guidance to improve its risk management posture. At the organization level, NTIA established security and privacy control metrics, assigned an impact level category for each of its spectrum IT systems, defined cyber risk management roles, and developed a continuous monitoring strategy. At the system level, NTIA has identified system stakeholders, documented the types of information processed, and defined and prioritized security and privacy requirements.

The purpose of the *categorize* step is to inform organizational risk management processes and tasks by determining the negative impact of cybersecurity threats to organizational operations and assets. With respect to the *categorize* step, NTIA has implemented all three categorization-related tasks for each of its legacy spectrum IT systems.[26] Specifically, for each of its legacy spectrum IT systems, NTIA

- documented system descriptions, including characteristics such as system purpose, classification status, and component applications;
- completed security categorizations identifying the types of data collected, processed, maintained, shared, or stored by the system, and weighting these data types by their impact levels;[27] and
- obtained approval from leadership (e.g., system owner, chief information officer, or IT program manager) on these security categorizations.

[26]We reviewed NTIA's implementation of system-level *prepare* and *categorize* tasks for the agency's legacy systems. NTIA has not yet progressed far enough in its modernization to be able to conduct NIST RMF tasks for its modernized systems.

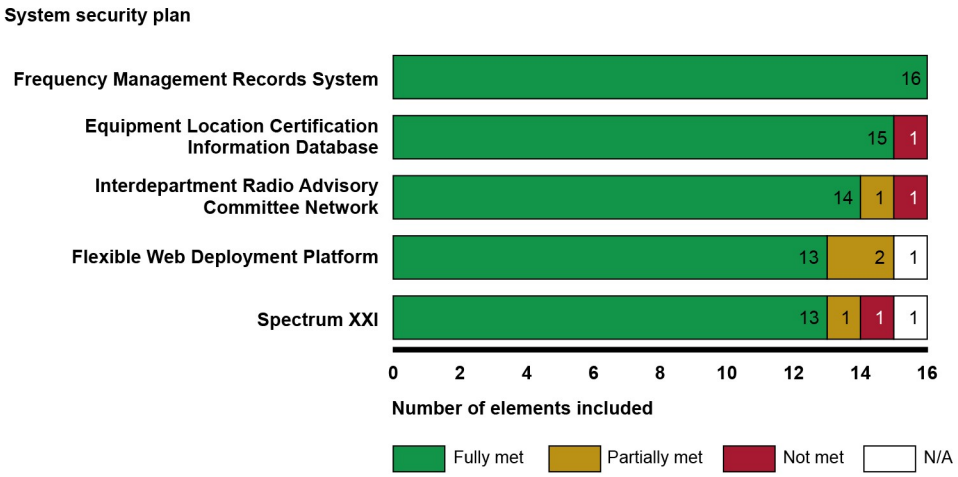
[27]According to NIST, a security categorization considers the potential adverse impacts of the loss of confidentiality, integrity, or availability of a system's data. See National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2 (Gaithersburg, MD: December 2018).

System Security Plans for NTIA Spectrum IT Systems Included Most but Not All Recommended Elements

System security plans (SSP) describe security requirements for a given system and the security controls in place or planned for meeting those requirements. NIST guidance recommends agencies develop SSPs according to 16 elements regarding both structure and content.[28] For example, SSPs are to include the system name, general description, and contacts; impact categorization across confidentiality, integrity, and availability; security controls; and evidence of both annual review and the changes made during such review.

NTIA maintains five SSPs covering its seven legacy systems.[29] For these plans, NTIA included all 16 elements recommended by NIST in its SSP for one system, and at least 13 of the 16 elements in each of the other four SSPs. Figure 5 shows our assessment of the content of NTIA's SSPs against the recommendations in NIST guidance.

Figure 5: Assessment of National Telecommunications and Information Administration (NTIA) Spectrum IT System Security Plan Elements



Source: GAO review of NTIA documentation. | GAO-25-107509

Accessible Data for Figure 5: Assessment of National Telecommunications and Information Administration (NTIA) Spectrum IT System Security Plan Elements

System security plan	Fully met	Partially met	Not met	N/A
Frequency management records system	16	0	0	0
Equipment location certification information database	15	0	1	0

[28]National Institute of Standards and Technology, *Guide for Developing Security Plans for Federal Information Systems*, Special Publication 800-18 (Gaithersburg, MD: February 2006).

[29]According to NTIA officials, since NTIA is in the beginning stages of its modernization efforts, it does not have fully devel oped system security plans for its modernized systems. Therefore, legacy systems' security plans remain the plans of record for these systems' security specifications.

System security plan	Fully met	Partially met	Not met	N/A
Interdepartment radio advisory commit-tee network	14	1	1	0
Flexible web deployment platform	13	2	0	1
Spectrum XXI	13	1	1	1

Source: GAO review of NTIA documentation. I GAO-25-107509

Notes: The system security plan (SSP) for the Flexible Web Deployment Platform covers the FreqCoord system and the Spectrum T ransition Tool, and the SSP for the Interdepartment Radio Advisory Committee Network covers the Data Capture and Forwarding System.
SSP information on system interconnection and information sharing were assessed as "N/A" because the associated systems are reported as having no interconnection relationships.

NTIA followed most NIST guidance regarding the information it contained within its SSPs, including details on system specifications and relevant security controls. However, NTIA did not include change logs, approval dates, and annual review documentation for all of its SSPs. Specifically:

- For three of its SSPs—the Equipment Location Certification Information Database, Interdepartment Radio Advisory Committee Network, and Spectrum XXI SSPs—NTIA did not document whether and when it had conducted an annual review of the SSP. This review includes logging any changes made, such as updated system contact information.
- For a fourth SSP, the Flexible Web Deployment Platform SSP, NTIA documentation indicated that an annual review had taken place, but did not include a change log specifying changes made.
- Three SSPs—the Flexible Web Deployment Platform, Interdepartment Radio Advisory Committee Network, and Spectrum XXI SSPs—included approval dates for the most recent version of the plan but did not include version numbers or what information changed between versions.

According to NTIA officials, its SSPs should maintain logs of changes resulting from annual reviews, and all recent reviews of SSPs should be documented in change logs that include the version number and the date of the change. Officials stated that NTIA uses a standard Department of Commerce tool to develop its SSP documents that does not have the functionality to document change logs, and that they have requested this functionality be added. NTIA officials also stated that the Department of Commerce has not yet established a time frame for when this functionality will be available to NTIA.

It is important that NTIA document annual reviews to ensure that the plan reflects the correct information about the system. Until NTIA maintains change logs that document evidence and results of annual reviews, officials cannot be sure that security reviews are based on fully accurate information.

NTIA Met Most but Not All Key Practices for Its Cloud Implementation

In prior work, GAO established six key practices for federal agencies to follow to improve their cloud security, based on a review of federal policies and practices and input from public and private sector experts.[30] These practices recommend that agencies

[30]Specifically, the six key practices are based on Office of Management and Budget cloud security policies and guidance from the General Services Administration, the Department of Homeland Security, and NIST. See GAO-23-105482.

- delineate security responsibilities between the agency and cloud service provider;[31]
- document identity, credential, and access management (ICAM) policies and procedures that identify user privileges and support separation of duties across systems;[32]
- develop and implement a plan for continuously monitoring the cloud system;[33]
- define security metrics in a service level agreement with the cloud service provider;[34]
- use Federal Risk and Authorization Management Program (FedRAMP) security guidance as part of granting cloud systems an authority to operate;[35] and
- document procedures for responding to and recovering from security incidents for the cloud system.[36]

According to NTIA officials, the agency began migrating its legacy systems to the cloud in 2022. As of September 2024, the migration of unclassified legacy systems is complete, and classified systems are expected to be migrated to the cloud by 2026. Officials further stated that cloud migration of spectrum IT systems was selected as the first step in its modernization process to establish a foundation that facilitates scalability and enhanced security, among other improvements.

Of the six key cloud security practices, NTIA fully met five and partially met one. Table 3 shows the extent to which NTIA has implemented each of the six key practices for cloud security.

[31]See Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019); and Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security Technical Reference Architecture* (Washington, D.C.: Aug. 2021).

[32]Office of Management and Budget, *Federal Zero Trust Strategy*, OMB Memorandum M-22-09 (Washington, D.C.: Jan. 2022); Office of Management and Budget, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, OMB Memorandum M-19-17 (Washington, D.C.: May 21, 2019); and OMB, *Federal Cloud Strategy*. National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing*, Special Publication 800-144 (Gaithersburg, MD: Dec. 2011); Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security*; and General Services Administration, *Federal Cloud Strategy Guide Agency Best Practices for Cloud Migration* (Washington, D.C.: Feb. 2021).

[33]FedRAMP Program Management Office, *FedRAMP Security Assessment Framework*, (Washington, D.C.: Nov. 2017); OMB, *Federal Cloud Strategy*; General Services Administration, *FedRAMP Agency Authorization Process: Reusing Authorizations for Cloud Products Quick Guide* (July 26, 2022), *https://www.fedramp.gov/documents-templates/*; Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security*; and National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD: Sept. 2020).

[34]OMB, *Federal Cloud Strategy*; Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security*; and General Services Administration, *Federal Cloud Strategy Guide*.

[35]Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 2011); Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security*; FedRAMP Program Management Office, *Security Assessment*; and General Services Administration, *Federal Cloud Strategy Guide*.

[36]OMB, *Security Authorization*; National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing*, Special Publication 800-144 (Gaithersburg, MD: Dec. 2011); Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security*; and General Services Administration, *Federal Cloud Strategy Guide*.

Table 3: Assessment of National Telecommunications and Information Administration (NTIA) Implementation of Key Practices for Cloud Security for Its Spectrum IT Systems

Key practice	Assessment	Description of assessment
Delineate security responsibilities between the agency and the cloud service provider for the cloud system	fully met criteria	NTIA identified its control implementation responsibilities as well as those of cloud service providers. For example, it has a control implementation summary that outlines the controls for which the provider is responsible versus those that remain the government customer's responsibility. It also has a customer responsibility matrix that outlines the provider's security responsibilities.
Document the identity, credential, and access management (ICAM) policies and procedures for the cloud system	partially met criteria	NTIA documented identity and authentication procedures for its cloud systems, including the use of multifactor authentication for organizational users of the cloud systems. However, NTIA did not fully document access control procedures that identified the authorized users of the systems, group and role membership, and access authorizations.
Develop and implement a plan for continuously monitoring the cloud system	fully met criteria	NTIA developed and implemented a plan for continuously monitoring the security controls it is required to monitor regarding its cloud service provider's activities and documented its review of related continuous monitoring reports.
Define security metrics in a service level agreement with the cloud service provider	fully met criteria	NTIA's service level agreement with the provider defined performance metrics and defined enforcement mechanisms to ensure the specified performance levels are achieved. For example, a credit is offered towards monthly service fees if service levels are not achieved.
Use the Federal Risk and Authorization Management Program (FedRAMP) when conducting risk assessments, security authorizations, and granting an authority to operate for the cloud system	fully met criteria	NTIA contracted with a provider authorized to operate under FedRAMP and documented the provider's compliance with FedRAMP security authorization requirements. NTIA documented the ongoing FedRAMP authorizations and authority to operate for each of the five systems. Security authorizations included an assessment of the risk level for each program.
Document procedures for responding to and recovering from security incidents for the cloud system	fully met criteria	NTIA documented procedures for responding to and recovering from cloud security-related incidents, including an incident response plan for its spectrum IT systems. Specifically, NTIA documented procedures instructing the system owner on how to coordinate with security operations and internal affairs to investigate and analyze the incident to determine the impact and criticality.

Legend:
● = The agency fully met the criteria.
◐ = The agency partially met criteria.
○ = The agency did not meet the criteria.

Source: GAO analysis of NTIA documentation. | GAO-25-107509

NTIA completed several actions to improve its cloud security practices. For example, it defined security control responsibilities for itself and its provider, developed a service level agreement to define metrics such as the level of detection and blocking of computer viruses, ensured provider compliance with FedRAMP by way of an authority to operate, and documented incident response and recovery procedures and plans.

NTIA also developed detailed lists of access roles and privileges for several of its core spectrum IT systems. However, it did not document access roles and privileges with the policies and procedures it developed for

each system. Specifically, while user roles are identified in the SSP for the IRACNet system, specific duties and associated access privileges for each role are not listed. Without an accurate and specific delineation of roles, improper privileges may be assigned to certain users.

According to NTIA officials, the agencywide access management policies and procedures it already has in place, combined with appropriate security controls, are sufficient to document role limitations for individual users. However, even if these policies and controls together are likely to minimize inappropriate access, it is important to unambiguously document specific system access privileges for each user role for use in decision making; for instance, to more quickly be able to determine access rights in the event of a breach. Until NTIA fully documents ICAM policies and procedures for each system that identify the authorized users of the system, group and role membership, and specific authorizations of access, the agency's spectrum IT systems may be at greater risk of unauthorized access.

NTIA Incorporated Leading Interagency Collaboration Practices but Lacks a Data Governance Plan

NTIA largely met leading practices for interagency collaboration through extensive coordination with its federal agency partners, for example, in defining common outcomes for planned functionality and delineating roles and responsibilities for each agency. NTIA also is developing a new data standard to facilitate its modernization and has obtained input from key stakeholders for its use. However, NTIA has not yet developed a data governance plan to document decisions regarding the new data standard, such as roles and responsibilities for making changes to the standard.

NTIA Incorporated Leading Practices for Enhancing Spectrum IT Collaboration with Agency Partners

Interagency collaboration involves collaboration or coordination between two or more federal entities, or within components of the same entity. For example, interagency working groups can establish governing structures and policies that have a high impact on organizational modernization. With respect to spectrum modernization, this can include mechanisms for accountability and policies that control spectrum management activities. In addition, leading interoperability guidance frameworks have emphasized that full operational interoperability requires shared governance structures that facilitate coordination between agency partners.[37] Among other things, GAO leading practices for interagency collaboration include defining common outcomes that clarify needed specific resources and skills, developing measures for shared accountability among group members, and clarifying roles and responsibilities for each member.[38]

NTIA generally incorporated the eight leading interagency collaboration practices in its spectrum IT modernization planning efforts. Among other things, NTIA:

[37]See, for example, data governance principles discussed in Cybersecurity and Infrastructure Security Agency, *Interoperability Continuum, A tool for improving emergency response communications and interoperability* (June 2021) and European Commission, *New European Interoperability Framework, Promoting seamless services and data flows for European public administrations* (2017).
[38]GAO-23-105520.

- **Defined common outcomes.** NTIA documented mission needs and the modernization's concept of operations with stakeholder input. These included the major challenges and opportunities for the modernization, such as automated system functionality and specific, time-based objectives for cloud migration.
- **Clarified roles and responsibilities.** NTIA documented roles and responsibilities for its spectrum management partners in its national spectrum security management plan, as well as in a procedural manual for frequency management.[39] For example, NTIA defined leadership roles and responsibilities within the IRAC for ensuring the interoperability of systems, such as committee and subcommittee heads and an elected chairperson. NTIA also delegated oversight over spectrum national security systems to several review boards, committees, and steering groups, and outlined a process for developing software that will support the modernized systems.
- **Leveraged resources and information.** NTIA documented its planned usage of staffing and funding to support the modernization. Additionally, NTIA uses IRACNet—its system responsible for facilitating IRAC proceedings—to collaborate with agencies and subcommittees, conduct meetings, and manage data.

More detailed information on our assessment of NTIA interagency collaboration practices can be found in appendix II.

NTIA Met Most but Not All Key Practices to Establish Governance Structures for Its New Data Standard

Data standards are critical for improving the interoperability, accessibility, and quality of spectrum data, replacing outdated technology, and enabling future automation goals. As we have previously reported, establishing a data governance structure is critical to ensuring that the integrity of data standards is maintained over time.[40]

Previous work by GAO and data standards-setting organizations, as well as policies and processes recommended by federal agencies, identified five key practices for agencies to follow in developing and approving data standards.[41] Among other things, these key practices recommend establishing definitions which describe each data element to ensure information is consistent and creating a data exchange standard with technical specifications which describe the format, structure, tagging, and transmission of each data element. Furthermore, they recommend that agencies should plan for and enforce consistent application of data standards and obtain input from stakeholders in establishing data standards.

NTIA is in the process of replacing its current standard, the Government Master File (GMF) Card Format, which, according to NTIA officials, has recently resulted in manual processes and lengthy delays. NTIA has developed a new standard, based on the GMF eXtensible Markup Language (XML), to replace its current standard.[42] According to NTIA officials, the GMF XML standard allows for greater flexibility by establishing a

[39]Department of Commerce National Telecommunications and Information Administration, *Manual of Regulations and Procedures for Federal Radio Frequency Management* (January 2021, revised January 2023).

[40]GAO, *DATA Act: Progress Made in Initial Implementation but Challenges Must be Addressed as Efforts Proceed*, GAO-15-752T (Washington, D.C.: July 29, 2015).

[41]GAO-19-284 and GAO-17-156.

[42]XML is a flexible, nonproprietary set of standards for tagging information so that it can be transmitted using internet protocols and readily interpreted by other computer systems.

common format for data to be shared, including through direct machine-to-machine transfer.[43] The GMF XML standard also makes use of a data dictionary—information on data elements, their definitions, descriptions, codes, and values—and indirectly manages and enforces consistent application of data standards because it does not allow data outside of specific parameters.

NTIA fully met three of the five key practices in developing and implementing its new data standard and partially met two. Table 4 summarizes details on the extent to which NTIA met each of the five key practices.

Table 4: Assessment of National Telecommunications and Information Administration (NTIA) Spectrum IT Implementation of Key Practices for Data Governance

Key practice	Assessment	Description of assessment
Developing and approving data standards for semantics and syntax	fully met criteria	NTIA built and promoted a data standard to enable the use of mission-critical data and decision making through utilization of the new Government Master File (GMF) eXtensible Markup Language (XML) data standard. To do so, NTIA built and promoted a comprehensive data inventory that improved data interoperability and accessibility. The NTIA GMF XML data specification documentation enables an improved data structure by outlining newly required data restrictions and values that data formatted under the schema must follow.
Managing, controlling, monitoring, and enforcing consistent application of data standards	fully met criteria	NTIA enforced consistent adherence to data standards and provided leadership on data usage considerations in its development of the GMF XML standard. For example, the standard has been set up to reject data values that do not meet pre-defined parameters.
Overseeing changes to existing data standards and resolving conflicts related to the application of data standards	partially met criteria	NTIA provided oversight to an external group with responsibility for making changes to its data standard, and incorporated input from this group on changes to data requirements, such as modified frequency assignment actions. However, it did not document how conflicts arising from the application of the data standard would be resolved.
Obtaining input from stakeholders and involving them in key decisions	fully met criteria	According to NTIA officials, NTIA worked with its spectrum IT partner agencies on the Interdepartment Radio Advisory Committee (IRAC) to obtain input on the data standard prior to its finalization. Additionally, NTIA has requested, received, and incorporated agency input on the level of compatibility with previous standards that agencies require GMF XML to have.
Delineating roles and responsibilities for decision-making and accountability, including roles and responsibilities for stakeholder input on key decisions	partially met criteria	NTIA delegated responsibility to the Frequency Assignment Subcommittee (FAS), an IRAC subcommittee, to make decisions regarding use of the data standard, for example in addressing frequency assignment issues brought before IRAC and in making improvements to the frequency assignment process. However, NTIA did not document this delegation or roles and responsibilities of those included in FAS.

Legend:

● = The agency fully met the criteria.

◐ = The agency partially met criteria.

○ = The agency did not meet the criteria.

Source: GAO analysis of NTIA documentation. | GAO-25-107509

NTIA has taken several steps to improve its data standard according to key practices. Among other things, the agency has regularly obtained input from stakeholders and involved them in key decisions regarding development of the new GMF XML data standard. NTIA also created a working group that allows partner

[43]Machine-to-machine data exchange refers to the automated exchange of information between computers without human involvement.

agencies to participate in key decisions related to the data standard. The working group also allows NTIA to more easily update partners on its future actions and plans. NTIA officials stated they are using a phased approach in moving to the new data standard so that affected agencies are comfortable with the new standard and related processes. NTIA has also solicited feedback from affected agencies on the GMF XML data standard's compatibility with previous standards.

However, NTIA only partially met key practices on overseeing changes to data standards and defining roles and responsibilities for stakeholders responsible for key decisions on these standards. Specifically, NTIA did not document how it resolves conflicts that arise from the use of its new data standard. Further, while NTIA delegates responsibilities regarding use of the new standard to the IRAC Frequency Assignment Subcommittee, it did not document in detail what responsibilities it delegated. It also has not delineated roles and responsibilities regarding compliance with the data standard.

Documentation of data governance-related decisions such as these in an agencywide plan for data governance is critical to ensuring the integrity of data standards, and compliance with them over time. While NTIA has plans to develop a data governance framework, as of February 2025, it has not established a specific time frame for developing one.

According to agency officials, NTIA plans to rely on the prime contractor of its overall modernization to develop its data governance plan and plans to establish a time frame for the development of the plan after task orders for the modernization contract have been developed. Given the progress and key decisions NTIA has already made in developing its new standard, it is important that NTIA centrally documents the data governance decisions it has made to better inform how it intends these standards to be used during the remainder of its modernization. Until it does so, NTIA and its partners may face issues in resolving conflicts related to the new data standard or in accountability to key decisions regarding the standard.

Conclusions

NTIA is planning to modernize its major spectrum IT systems by 2030 to update outdated legacy systems and improve its efficiency in allocating and managing the use of spectrum. NTIA has taken several important actions but has yet to develop several key planning documents that would assist it in preparing for the remainder of its modernization. The agency has met most cybersecurity practices for risk management, systems security, and cloud security. However, it did not fully develop organization-wide risk management documentation and system security plans in accordance with NIST guidance, nor did it document access control procedures for the cloud instances of its systems. Without fully documenting information on the cybersecurity of its systems, NTIA runs the risk of miscommunication in understanding its security posture, and in making decisions on how to modernize these systems.

NTIA has made progress in developing a new data standard to improve the interoperability of its spectrum IT systems as it proceeds with their modernization. However, the agency is deferring development of a data governance plan with details on key procedures, roles, and responsibilities for the new standard until a related contract is in place. Without a common understanding of these details, NTIA may face delays in fully implementing its new standard.

Recommendations for Executive Action

We are making five recommendations to NTIA:

The NTIA Administrator should direct the IT Division in the Office of Policy Coordination and Management to work with the Office of Spectrum Management to develop an organizational risk management strategy that includes a determination of organizational risk tolerance, acceptable risk assessment methodologies, and details on strategies for responding to risks (such as risk acceptance, mitigation, or avoidance). (Recommendation 1)

The NTIA Administrator should direct the IT Division in the Office of Policy Coordination and Management to work with the Office of Spectrum Management to develop an organizational risk assessment that leverages aggregated information from system-level risk assessment results and risk considerations relevant at the organization level. (Recommendation 2)

The NTIA Administrator should direct the IT Division in the Office of Policy Coordination and Management to work with the Department of Commerce and the NTIA Office of Spectrum Management to ensure and document that system security plans for NTIA's spectrum IT systems are reviewed, at a minimum, annually, and include logs detailing the date of review and resulting changes. (Recommendation 3)

The NTIA Administrator should direct the IT Division in the Office of Policy Coordination and Management to work with the Office of Spectrum Management to fully document identity, credential, and access management procedures for its cloud systems, including identification of authorized users and their roles, and associated access privileges, for each of its spectrum IT legacy systems. (Recommendation 4)

The NTIA Administrator should direct the IT Division in the Office of Policy Coordination and Management to work with the Office of Spectrum Management to specify a time frame for developing a data governance plan that resolves conflicts related to the application of NTIA's new data standard and defines roles and responsibilities for making decisions regarding the standard. (Recommendation 5)

Agency Comments and Our Evaluation

We provided a draft of this report for review and comment to NTIA, the agency to which we made recommendations. In an email response, an official in NTIA's Office of Chief Counsel stated that NTIA concurred with our five recommendations and that the agency will prepare a formal action plan to implement them. NTIA also provided further information regarding recommendation 2. This recommendation stated that NTIA should complete a risk assessment at an organization-wide level that centrally incorporates information from spectrum IT system-level risk assessment results. As part of its comment response, NTIA provided documentation on steps the agency has taken regarding our related finding, including a listing of attributes for some agencywide risks, such as impact level and mitigation strategy category. The agency also provided charts associated with the listing that included metrics on impact and number of risks aggregated at an NTIA program level. This evidence indicates that NTIA has undertaken efforts to aggregate and monitor individual risks at a wider level.

However, the additional evidence provided by NTIA does not fully demonstrate an assessment of organization-level risks in line with NIST RMF guidance. Such an assessment would include, for example, whether higher-impact systems are segregated from lower-impact systems and specifics on what actions are entailed by each agencywide mitigation designation. It is also unclear how this information is used by NTIA as part of a broader assessment of the agency's risks. Therefore, we continue to believe that our recommendation is valid. By implementing it, NTIA can ensure the agency is able to identify and track progress in mitigating its most impactful cyber risks.

We also provided a draft for comment to DOD. In an email response, an official in DOD's Performance Improvement Directorate stated that DOD concurred with our report and had no additional comments.

We are sending copies of this report to the appropriate congressional committees, the Administrator of NTIA, the Secretary of Commerce, the Secretary of Defense, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at dsouzav@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

//SIGNED//

Vijay A. D'Souza
Director, Information Technology and Cybersecurity

List of Committees

The Honorable Roger Wicker
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Ted Cruz
Chairman
The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Brett Guthrie
Chairman
The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine the extent to which the National Telecommunications and Information Administration (NTIA) plans to modernize its spectrum IT infrastructure incorporated leading practices for cybersecurity and (2) determine the extent to which NTIA plans to modernize its spectrum IT infrastructure incorporated leading practices for interoperability.

To address the first objective, we assessed NTIA plans and practices that are critical components of its modernization planning efforts against leading practices for cybersecurity. Specifically:

To evaluate NTIA's risk management plans, we selected the first two risk management steps from the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) that we deemed critical for cybersecurity planning, known as the *prepare* and *categorize* steps.[1]

- The purpose of the prepare step is to carry out essential activities at the organization and system level to enable the organization to manage its cybersecurity risks using the risk management framework.
- The purpose of the categorize step is to inform organizational risk management processes and tasks by determining the negative impact of cybersecurity threats to organizational operations and assets.

These steps are considered critical because they facilitate system readiness for the execution of the remaining risk management objectives. We compared NTIA plans and practices against these steps to determine whether NTIA took steps to improve its posture for managing security and privacy risks.

For the *prepare* step, we compared NTIA plans and practices against five required organization-level practices.[2] NTIA has not yet progressed far enough in its modernization to complete these steps for each of its modernized systems.[3] Also, system-specific *prepare* actions were not yet a part of the NIST risk management framework at the time NTIA's legacy systems were created. Since actions within the *categorize* step focus on the creation of system-specific plans, we analyzed completion of the three *categorize* tasks against NIST guidance at an individual system level for each of NTIA's legacy systems.[4]

- To evaluate NTIA's system security plans (SSP), we analyzed five NTIA SSPs that together encompass security plan information for NTIA's seven legacy spectrum IT systems. We compared the content of these SSPs against NIST guidance to determine whether NTIA documented 16 key pieces of information needed to evaluate the security of its systems.[5]

[1]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2 (Gaithersburg, MD: December 2018).

[2]Two of the organization-level practices within the *prepare* step of NIST guidance are optional practices.

[3]NTIA plans to modernize its legacy systems over a nine-year period (fiscal years 2022 through 2030), during which these systems will remain in place. Since NTIA does not have fully developed cybersecurity-related plans for its modernized systems, legacy systems' documentation must still be both current and complete.

[4]We analyzed completion of the three *categorize* tasks across four systems: Spectrum XXI; the Interdepartment Radio Advisory Committee Network system, of which the Data Capture and Forwarding System is a sub-system; the Equipment Location Certification Information Database; and the Flexible Web Deployment Platform, of which the FreqCoord system and the Spectrum Transition Tool are sub-systems.

[5]National Institute of Standards and Technology, *Guide for Developing Security Plans for Federal Information Systems*, Special Publication 800-18, Revision 1 (Gaithersburg, MD: February 2006).

- To evaluate NTIA's cloud security practices, we used six key practices and 17 corresponding sub-practices for securing cloud systems previously selected by GAO based on a review of federal policies and guidance and with assistance from two panels of experts from the public and private sectors.[6] We compared NTIA and cloud service provider documentation—such as NTIA policy documents and SSPs and control implementation and customer responsibility worksheets used by providers—against each of the 17 sub-practices to determine whether NTIA documented key decisions, plans, and roles for securing its cloud migration.

In selected instances where NTIA had not made sufficient progress to perform a complete analysis, we compared documentation on NTIA legacy systems against the cybersecurity practices.

To address the second objective, we evaluated information in NTIA plans, policies, and other modernization-related documentation on interagency collaboration and data standards to inform the extent to which NTIA's modernization planning would facilitate greater interoperability between its systems and those of its users.[7] We considered adherence to these leading practices as a reasonable representation of the status of organizational interoperability planning, since full operational interoperability depends on shared governance structures facilitated by cross-agency coordination.

In particular, we assessed NTIA interagency collaboration actions against eight selected leading practices developed in prior GAO work with the assistance of public and private-sector experts, to evaluate NTIA's actions to coordinate with its federal agency partners in planning modernization of its spectrum IT systems.[8] We assessed incorporation of these leading practices based on key considerations under each practice and modified or excluded some key considerations to suit our interoperability objective or the specific circumstances of NTIA's modernization.

We also evaluated NTIA's plans for developing and implementing data standards that support interoperability. To do so, we used five key practices for data governance structures, which we identified in our previous work based on leading models for data governance and actions endorsed by standards-setting organizations, and policies and procedures recommended by federal agencies.[9] We then compared NTIA data standards and data governance documentation against these key practices to evaluate NTIA actions taken to coordinate development of its standard.

We supplemented our analyses with interviews of relevant officials within NTIA's Office of Spectrum Management and the IT Division within NTIA's Office of Policy Coordination and Management regarding their

[6]GAO, *Cloud Security: Selected Agencies Need to Fully Implement Key Practices*, GAO-23-105482 (Washington, D.C.: May 18, 2023).

[7]The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 defines a covered agency as the Department of Defense as well as any federal entity that the Assistant Secretary of Commerce for Communications and Informati on—the Administrator of NTIA—determines is appropriate. Pub. L. No. 116-283, § 9203(e)(1), 134 Stat. 4797. NTIA chairs the Interdepartment Radio Advisory Committee (IRAC), which includes a variety of subcommittees that have specialized functions, s uch as assisting NTIA in assigning frequencies. The IRAC consists of NTIA and the following entities: Departments of Agriculture, Commerce, Defense (including the Air Force, Army, and Navy), Energy, Homeland Security, Interior, Justice, State, Transportation, Treasury, and Veterans Affairs, as well as the Federal Aviation Administration, National Aeronautics and Space Administration, National Scie nce Foundation, U.S. Agency for Global Media, U.S. Coast Guard, and U.S. Postal Service. NTIA also designated the Federal Communications Commission, a liaison to the IRAC, as a covered agency.

[8]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 24, 2023).

[9]GAO, *DATA Act: OMB Needs to Formalize Data Governance for Reporting Federal Spending*, GAO-19-284 (Washington, D.C.: Mar. 22, 2019); and *DATA Act: OMB and Treasury Have Issued Additional Guidance and Have Improved Pilot Design but Implementation Challenges Remain*, GAO-17-156 (Washington, D.C.: Dec. 8, 2016).

spectrum IT modernization planning efforts. For each assessment, we determined, based on the documents and data provided, the extent to which NTIA had fully met, partially met, or not met the required tasks or activities. We considered a criterion to be

- fully met when the documentation provided by NTIA addressed all tasks or activities associated with the key or leading practice;
- partially met when the documentation provided by NTIA addressed some, but not all, tasks or activities associated with the key or leading practice; and
- not met when the documentation provided by NTIA did not address any tasks or activities associated with the key or leading practice.

We conducted this performance audit from April 2024 to May 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Assessment of NTIA Spectrum IT Modernization Plans Against GAO's Leading Practices for Interagency Collaboration

We assessed the National Telecommunications and Information Administration's (NTIA) plans and practices for its spectrum IT modernization against eight leading practices for interagency collaboration developed in prior GAO work.[1] We determined that NTIA generally incorporated all eight leading practices for interagency collaboration, as shown in table 5.

Table 5: Assessment of National Telecommunications and Information Administration (NTIA) Spectrum IT Implementation of GAO's Leading Practices for Interagency Collaboration

Leading practice	Assessment	Key considerations used[a]	Description of assessment
Define common outcomes	generally incorporated key considerations	Have the crosscutting challenges or opportunities been identified?	NTIA has defined planned long-term outcomes, as well as major opportunities and challenges for its cloud migration. For example, the concept of operations (CONOPS) document lists future capabilities of the modernization, such as an integrated, searchable manual and an enhanced information-sharing capacity for Interdepartment Radio Advisory Committee (IRAC) management. NTIA distributed the CONOPS to agency partners and sought feedback.
Define common outcomes	generally incorporated key considerations	Have short- and long-term outcomes been clearly defined?	NTIA has defined planned long-term outcomes, as well as major opportunities and challenges for its cloud migration. For example, the concept of operations (CONOPS) document lists future capabilities of the modernization, such as an integrated, searchable manual and an enhanced information-sharing capacity for Interdepartment Radio Advisory Committee (IRAC) management. NTIA distributed the CONOPS to agency partners and sought feedback.
Define common outcomes	generally incorporated key considerations	Have the outcomes been reassessed and updated, as needed?	NTIA has defined planned long-term outcomes, as well as major opportunities and challenges for its cloud migration. For example, the concept of operations (CONOPS) document lists future capabilities of the modernization, such as an integrated, searchable manual and an enhanced information-sharing capacity for Interdepartment Radio Advisory Committee (IRAC) management. NTIA distributed the CONOPS to agency partners and sought feedback.

[1]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 24, 2023).

Leading practice	Assessment	Key considerations used[a]	Description of assessment
Ensure accountability	generally incorporated key considerations	What are the ways to monitor, assess, and communicate progress toward the short- and long-term outcomes?	NTIA is implementing an acquisition strategy required in the Commerce Acquisition Manual for its modernization, which provides policies and guidance that NTIA must follow to conduct an acquisition, in addition to providing a framework that all high-dollar acquisition projects must follow. As required by this framework, NTIA modernization program managers communicate progress and receive approval from NTIA and Commerce review boards before moving to subsequent development phases. NTIA also provides regular quarterly updates on the status of spectrum IT modernization and next steps to external stakeholders such as the Spectrum Modernization IT Working Group.
Bridge organizational cultures	generally incorporated key considerations	Have strategies to build trust among participants been developed?	To build trust among its spectrum IT partners, NTIA developed a stakeholder management plan that required the setup of regular stakeholder input meetings, a forum for federal partner agencies to offer their perspectives on ongoing NTIA initiatives. Additionally, NTIA officials stated they are rolling out the modernization at an intentionally slower pace to ensure that agencies feel comfortable acclimating to the new processes and standards. Further, NTIA has defined common spectrum-related terminology and definitions, which reduces miscommunication among participating agencies.
Bridge organizational cultures	generally incorporated key considerations	Have participating agencies agreed on common terminology and definitions?	To build trust among its spectrum IT partners, NTIA developed a stakeholder management plan that required the setup of regular stakeholder input meetings, a forum for federal partner agencies to offer their perspectives on ongoing NTIA initiatives. Additionally, NTIA officials stated they are rolling out the modernization at an intentionally slower pace to ensure that agencies feel comfortable acclimating to the new processes and standards. Further, NTIA has defined common spectrum-related terminology and definitions, which reduces miscommunication among participating agencies.
Identify and sustain leadership	generally incorporated key considerations	Has a lead agency or individual been identified?	NTIA established the Spectrum National Security Systems (SNSS) Program Management Office within its Office of Spectrum Management in December 2018 to plan and lead all aspects of its modernization project. The SNSS office developed a management plan that states the office is to manage and evaluate the Office of Spectrum Management's mission and related capabilities required to support SNSS. The management plan also outlines the responsibility of all projects, NTIA staff, and contractors aligned with SNSS to keep the program on schedule and within budget and mitigate and manage risks.
Identify and sustain leadership	generally incorporated key considerations	How will leadership be sustained over the long term?	NTIA established the Spectrum National Security Systems (SNSS) Program Management Office within its Office of Spectrum Management in December 2018 to plan and lead all aspects of its modernization project. The SNSS office developed a management plan that states the office is to manage and evaluate the Office of Spectrum Management's mission and related capabilities required to support SNSS. The management plan also outlines the responsibility of all projects, NTIA staff, and contractors aligned with SNSS to keep the program on schedule and within budget and mitigate and manage risks.

Leading practice	Assessment	Key considerations used[a]	Description of assessment
Clarify roles and responsibilities	generally incorporated key considerations	Has NTIA identified stakeholder and agency roles and responsibilities as they relate to interoperable systems?	NTIA took several steps to clarify roles and responsibilities for spectrum IT-related activities. For example, it defined responsibilities for each IRAC participant in its manual of spectrum management procedures and regulations. NTIA directs IRAC to advise the Administrator of NTIA on frequency assignment coordination and spectrum policy development. NTIA also issued a management plan which directs the SNSS program manager to make decisions on NTIA planning and execution activities under executive oversight with input from various bodies, such as the NTIA IT Review Board, the Commerce IT Review Board, and IRAC.
Clarify roles and responsibilities	generally incorporated key considerations	Has a process for making decisions been agreed upon?	NTIA took several steps to clarify roles and responsibilities for spectrum IT-related activities. For example, it defined responsibilities for each IRAC participant in its manual of spectrum management procedures and regulations. NTIA directs IRAC to advise the Administrator of NTIA on frequency assignment coordination and spectrum policy development. NTIA also issued a management plan which directs the SNSS program manager to make decisions on NTIA planning and execution activities under executive oversight with input from various bodies, such as the NTIA IT Review Board, the Commerce IT Review Board, and IRAC.
Include relevant participants	generally incorporated key considerations	Have all relevant participants been included?	NTIA designated the agencies that are part of the IRAC as covered agencies under the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA) provisions on modernizing spectrum IT enabling easier coordination and sharing of information in areas such as frequency management.[b] NTIA also established a working group for spectrum IT modernization composed of representatives from these covered agencies. For each covered agency, NTIA documentation specifies requirements for participants in the working group, such as an ability to speak in detail on their agencies' activities and objectives.
Include relevant participants	generally incorporated key considerations	Do the participants have the appropriate knowledge, skills, and abilities to contribute?	NTIA designated the agencies that are part of the IRAC as covered agencies under the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA) provisions on modernizing spectrum IT enabling easier coordination and sharing of information in areas such as frequency management.[b] NTIA also established a working group for spectrum IT modernization composed of representatives from these covered agencies. For each covered agency, NTIA documentation specifies requirements for participants in the working group, such as an ability to speak in detail on their agencies' activities and objectives.
Leverage resources and information	generally incorporated key considerations	How will the collaboration be resourced through staffing?	NTIA leverages information, staffing, and funding resources in several ways. For example, the Administrator of NTIA serves as the Chair of the Interagency Spectrum Advisory Council, a forum for agencies to advise NTIA on spectrum-related policies. In this capacity, the Administrator can designate Vice Chairs to serve as the Chair in their absence or conduct certain Council-related activities. Additionally, NTIA obtained approval to use Commerce's Nonrecurring Expenses Fund to support the modernization. Further, NTIA leverages tools such as the Interdepartment Radio Advisory Committee Network to collaborate with agencies and subcommittees, facilitate meetings, and manage data.

Leading practice	Assessment	Key considerations used[a]	Description of assessment
Leverage resources and information	generally incorporated key considerations	How will the collaboration be resourced through funding? If interagency funding is needed, is it permitted?	NTIA leverages information, staffing, and funding resources in several ways. For example, the Administrator of NTIA serves as the Chair of the Interagency Spectrum Advisory Council, a forum for agencies to advise NTIA on spectrum-related policies. In this capacity, the Administrator can designate Vice Chairs to serve as the Chair in their absence or conduct certain Council-related activities. Additionally, NTIA obtained approval to use Commerce's Nonrecurring Expenses Fund to support the modernization. Further, NTIA leverages tools such as the Interdepartment Radio Advisory Committee Network to collaborate with agencies and subcommittees, facilitate meetings, and manage data.
Leverage resources and information	generally incorporated key considerations	How is NTIA using tools to better share information with covered agencies?	NTIA leverages information, staffing, and funding resources in several ways. For example, the Administrator of NTIA serves as the Chair of the Interagency Spectrum Advisory Council, a forum for agencies to advise NTIA on spectrum-related policies. In this capacity, the Administrator can designate Vice Chairs to serve as the Chair in their absence or conduct certain Council-related activities. Additionally, NTIA obtained approval to use Commerce's Nonrecurring Expenses Fund to support the modernization. Further, NTIA leverages tools such as the Interdepartment Radio Advisory Committee Network to collaborate with agencies and subcommittees, facilitate meetings, and manage data.
Develop and update written guidance and agreements	generally incorporated key considerations	If appropriate, have agreements regarding the collaboration been documented? A written document can incorporate agreements reached for any or all of the practices.	NTIA maintains an interconnection security agreement with the Federal Communications Commission, which uses its own IT to interact with NTIA IT. Additionally, NTIA and the Department of Defense have a use agreement in place for the Defense Information Systems Agency to provide Spectrum XXI maintenance and have a dash-8 (an option to extend services) in place to extend this agreement.
Develop and update written guidance and agreements	generally incorporated key considerations	Have ways to continually update or monitor written agreements been developed?	NTIA maintains an interconnection security agreement with the Federal Communications Commission, which uses its own IT to interact with NTIA IT. Additionally, NTIA and the Department of Defense have a use agreement in place for the Defense Information Systems Agency to provide Spectrum XXI maintenance and have a dash-8 (an option to extend services) in place to extend this agreement.

Legend:

● = The agency generally incorporated the associated key considerations.

◐ = The agency incorporated some but not all of the associated key considerations.

○ = The agency did not incorporate any of the associated key considerations.

Source: GAO analysis of NTIA documentation. | GAO-25-107509

[a]We modified or excluded some key considerations to suit our interoperability objective or the specific circumstances of NTIA's modernization.

[b]The FY21 NDAA defines a covered agency as the Department of Defense as well as any federal entity that the Assistant Secretary of Commerce for Communications and Information—the Administrator of NTIA—determines is appropriate. The IRAC consists of NTIA and the following entities: Departments of Agriculture, Commerce, Defense (including the Air Force, Army, and Navy), Energy, Homeland Security, Interior, Justice, State, Transportation, Treasury, and Veterans Affairs, as well as the Federal Aviation Administration, National Aeronautics and Space Administration, National Science Foundation, U.S. Agency for Global Media, U.S. Coast Guard, and U.S. Postal Service. NTIA also designated the Federal Communications Commission, a liaison to the IRAC, as a covered agency.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Vijay A. D'Souza, dsouzav@gao.gov

Staff Acknowledgments

Principal contributors to this report were Shaun Byrnes (Assistant Director), Ash Sabine Harper (Analyst in Charge), Umesh Thakkar (Analyst in Charge), Alexander Engel, Donna Epler, Smith Julmisse, Sachin Mirajkar, and Curt Williams. Other key contributors included Amanda Andrade, Tommy Baril, Jr., Miguel Cortez, Jr., Joe Kirschbaum, Michael Lebovitz, Kara Marshall, Nalylee Padilla, Andrew Stavisky, Michael Sweet, Sarah Veale, and Andrew Von Ah.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us