United States Government Accountability Office

Testimony

Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. ET
Wednesday, June 5, 2024

CYBERSECURITY

Efforts Initiated to Harmonize Regulations, but Significant Work Remains

Accessible Version

Statement of David B. Hinchman,
Director, Information Technology and Cybersecurity

GAO-24-107602

GAO Highlights

View GAO-24-107602. For more information, contact David B. Hinchman at (214) 777-5719 or HinchmanD@gao.gov.
Highlights of GAO-24-107602, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

June 5, 2024

CYBERSECURITY

Efforts Initiated to Harmonize Regulations, but Significant Work Remains

Why GAO Did This Study

Cyber-based intrusions and attacks on both federal and nonfederal systems by malicious actors are becoming more common and more disruptive. These attacks threaten the continuity, confidence, integrity, and accountability of essential systems. Moreover, the risks to these systems—including insider threats from witting or unwitting employees, mounting threats from around the globe, and the rise of new and more destructive attacks—collectively threaten to compromise sensitive data and destabilize critical operations.

GAO initially identified cybersecurity as a High-Risk area in 1997 and expanded it in 2003 to include critical infrastructure cybersecurity. Due to the persistent threat and need for urgent action, GAO continues to view the area as high risk.

Because the private sector owns most of the nation's critical infrastructure, it is vital that the public and private sectors work together to protect these assets and systems. However, according to ONCD, when critical infrastructure sectors are subject to multiple cybersecurity regulations, the result can be conflicting guidance, inconsistencies, and redundancies.

GAO was asked to testify on harmonizing cybersecurity regulations. This testimony summarizes the Administration's current efforts to address cybersecurity regulatory harmonization.

This statement is based on prior GAO reports and public information, as of May 2024, regarding the Administration's plans to harmonize regulations.

What GAO Found

Harmonization refers to the development and adoption of more consistent standards and regulations. Such consistency is important when critical infrastructure sectors are subject to multiple cybersecurity regulations. According to the White House, harmonizing regulatory requirements can lead to better security outcomes at lower costs.

Without harmonization, adverse impacts can occur. For example, GAO reported in 2020 that four federal agencies had established cybersecurity requirements for states to follow in securing data. However, these requirements had conflicting

parameters such as the number of unsuccessful log-on attempts prior to locking out users. The percentage of total requirements with conflicting parameters ranged from 49 percent to 79 percent. Slightly more than half of state officials surveyed said that such requirements led to a great increase or very great increase in the time and staff hours needed to address the conflicts. GAO made 12 recommendations to agencies; eight of them are implemented and four are not including two priority ones to the Office of Management and Budget to ensure agencies collaborate on requirements and state cybersecurity assessments.

Recognizing the importance of harmonizing cybersecurity regulations for our nation's critical infrastructure sectors, the Administration and Congress have begun relevant initiatives.

- **National cybersecurity strategy and implementation plan.** In March 2023 and July 2023, respectively, the White House released the National Cybersecurity Strategy and an accompanying implementation plan. Among other things, the strategy and implementation plan identified the need to establish an initiative on cyber regulatory harmonization but did not provide a time frame for completing subsequent actions to harmonize regulations.
- **Request for information on cybersecurity regulation harmonization.** In August 2023, the Office of the National Cyber Director (ONCD) issued a request for information seeking input on challenges with cybersecurity regulatory overlap and received over 100 public comments. ONCD has not published a summary of the comments.
- **National security memorandum on critical infrastructure security and resilience.** In April 2024, the Administration released *National Security Memorandum-22 on Critical Infrastructure Security and Resilience*. The memorandum calls for the Department of Homeland Security (DHS) to develop a plan to harmonize cybersecurity regulations as part of a national plan for infrastructure risk management, which is to be issued by April 2025.
- **Cyber incident reporting legislation.** The Cyber Incident Reporting for Critical Infrastructure Act was enacted in 2022 to help prioritize efforts to combat cyber threats by requiring certain entities to submit cyber incident reports to DHS. Pursuant to the act, in September 2023, DHS issued a report with eight recommendations and three proposed legislative changes to streamline and harmonize cyber incident reporting.

These key initial steps can inform the broader effort to harmonize cybersecurity regulations. Following through and executing specific plans and meeting established time frames are essential to achieving harmonization.

Chairman Peters, Ranking Member Paul, and Members of the Committee:

Thank you for the opportunity to discuss our work on the cybersecurity challenges that are impacting our nation's critical infrastructure. Our nation increasingly depends on computer-based information systems and electronic data to execute fundamental operations and to process, maintain, and report crucial information. Further, nearly all federal and nonfederal operations, including the nation's critical infrastructure, are supported by these systems and data.[1] Consequently, the safety of these systems and data is critical to public confidence and the nation's security, success, and welfare.

However, cyber-based intrusions and attacks on both federal and nonfederal systems by malicious actors are becoming more common and more disruptive. These attacks threaten the continuity, confidence, integrity, and accountability of these essential systems. Moreover, the risks to these systems—including insider threats from witting or unwitting employees, mounting threats from around the globe, and the rise of new and more destructive attacks—collectively threaten to compromise sensitive data and destabilize critical operations.

Because the private sector owns the majority of the nation's critical infrastructure, it is vital that the public and private sectors work together to protect these assets and systems. Toward this end, various federal agencies are responsible for assisting the private sector in protecting critical infrastructure, including enhancing cybersecurity. However, according to the Office of the National Cyber Director (ONCD), when critical infrastructure sectors are subject to multiple cybersecurity regulations, this can result in conflicting guidance, inconsistencies, and redundancies.[2] According to the White House, harmonizing regulatory

[1]The term "critical infrastructure" as defined in the Critical Infrastructures Protection Act of 2001 refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[2]Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations, 88 Fed. Reg. 55,694 (Aug. 16, 2023).

requirements can lead to better security outcomes at lower costs. The Administration has recently taken initial steps towards harmonizing and streamlining cybersecurity regulations to help address such concerns.

My statement today will discuss our past reporting and the Administration's recent work to harmonize cybersecurity regulations. To review the status of these efforts, we relied on prior GAO reports and public information, as of May 2024, regarding the Administration's harmonization plans and the impact of those plans on improving the nation's cybersecurity.

We conducted the work on which this statement is based 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

GAO has identified cybersecurity as a government-wide high-risk area for more than 25 years. Recognizing a growing threat, we first designated information security as a government-wide high-risk area in 1997. Subsequently in 2003, we expanded the information security high-risk area to include the cybersecurity of critical infrastructure. We further expanded this high-risk area in 2015 to include protecting the privacy of personally identifiable information.[3]

In September 2018, as part of our High-Risk Series, we identified four major cybersecurity challenges and 10 critical actions that the federal government and other entities need to take to address those challenges.[4] The major challenges are: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cybersecurity of critical infrastructure, and (4) protecting privacy and sensitive data. Figure 1 provides an overview of

[3]In general, personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and Social Security number; or that otherwise can be linked to an individual.

[4]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

the major challenges and the critical actions needed to address these challenges.

Figure 1: Four Major Cybersecurity Challenges and 10 Associated Critical Actions

Establishing a comprehensive cybersecurity strategy and performing effective oversight	Securing federal systems and information	Protecting cyber critical infrastructure	Protecting privacy and sensitive data
1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	5 Improve implementation of government-wide cybersecurity initiatives.	8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).	9 Improve federal efforts to protect privacy and sensitive data.
2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).	6 Address weaknesses in federal agency information security programs.		10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.
3 Address cybersecurity workforce management challenges.	7 Enhance the federal response to cyber incidents.		
4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).			

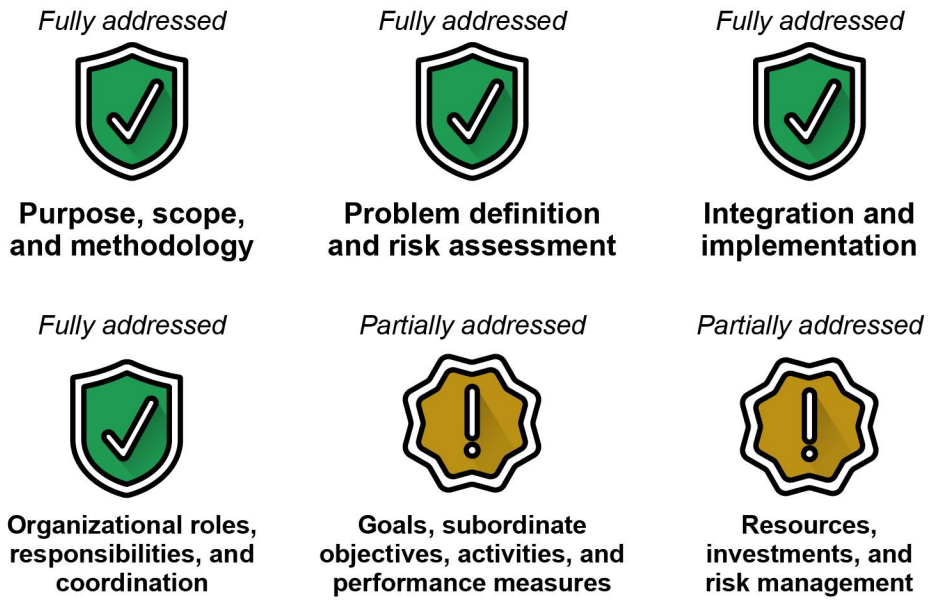
Sources: GAO (analysis and icons), Who is Danny (blue image); Gorodenkoff/stock.adobe.com (green image); metamorworks/stock.adobe.com (yellow image); Monster Ztudio/stock.adobe.com (red image); motorama/stock.adobe.com (icons); https://www.whitehouse.gov (logo). | GAO-24-107602

In our most recent update on this high-risk area in April 2023, we reiterated that fully establishing and implementing a national cybersecurity strategy was needed to protect the nation's information

systems and infrastructure.[5] We plan to further update this important area in the summer of 2024.

More recently, we reported on the Administration's efforts to establish and implement the National Cybersecurity Strategy.[6] Specifically, in February 2024 we found that that the strategy and its July 2023 implementation plan fully addressed four of six desirable characteristics of a national strategy, as identified in our prior work, and partially addressed the other two (see fig. 2).

Figure 2: Extent to Which the March 2023 National Cybersecurity Strategy and July 2023 Implementation Plan Addressed GAO's Desirable Characteristics of a National Strategy



Sources: GAO (analysis and yellow icon); YEVHENIIA/stock.adobe.com (green icon). | GAO-24-107602

For the partially addressed characteristics, the strategy and its implementation plan did not describe:

- *Outcome-oriented performance measures* that assess the extent to which initiatives are achieving outcome-oriented objectives, such as

[5]GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

[6]GAO, *Cybersecurity: National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy*, GAO-24-106916 (Washington, D.C.: Feb. 1, 2024).

improving information sharing or modernizing federal agency defenses. ONCD staff said it was not yet realistic to develop outcome-oriented measures, because such measures did not currently exist in the cybersecurity field in general. However, we believe it is feasible to develop such measures where applicable. For example, regarding the key initiative of disrupting ransomware attempts, the Department of the Treasury already collects information on the number and dollar value of ransomware-related incidents—for 2021 the reported total dollar value was about $886 million. This demonstrates that developing such measures is feasible and can be used for measuring effectiveness.

- *Resources and estimated costs* associated with the strategy, such as budgetary, human capital, IT, research/development, and contracts. While the implementation plan outlined initiatives that require executive visibility and interagency coordination, it did not identify how much it will cost to implement the initiatives. ONCD staff said estimating the cost to implement the entire strategy was unrealistic. However, while certain initiatives may not warrant a specific cost estimate, other activities supporting some of the key initiatives with potentially significant costs justify the development of a cost estimate. Such cost estimates are essential to effectively managing programs.

We concluded that without actions to address these shortcomings, ONCD will likely lack information on plan outcomes and encounter uncertainty on funding of activities. Consequently, we made two recommendations to ONCD to (1) assess initiatives that lend themselves to outcome-oriented measures and develop such performance measures for these initiatives and (2) estimate the costs of implementation activities. ONCD partially agreed with our finding on outcome-oriented measures and agreed with the related recommendation to assess the initiatives to identify those that warrant outcome-oriented performance measures. ONCD disagreed with our finding and associated recommendation that the strategy and implementation plan did not include specific details on the estimated cost of the plan's initiatives. Both of these recommendations remain open.

In addition, over the past few years, we have issued numerous reports that identified concerns resulting from varying cybersecurity requirements and the implementation of those requirements. For example:

- In February 2018, we reported on what was known about the extent to which critical infrastructure sectors had adopted the National Institute of Standards and Technology's (NIST) Framework for Improving

Critical Infrastructure Cybersecurity.[7] We found that most of the 16 critical infrastructure sectors took action to facilitate adoption of the framework. In addition, 12 of the 16 sectors developed guidance for implementing the framework. Nevertheless, we reported that federal and nonfederal officials identified four challenges to framework adoption.

Specifically, some entities may face regulatory, industry, and other requirements that could inhibit their adoption of the framework. We made nine priority recommendations that methods be developed for determining framework adoption by sector risk management agencies across their respective sectors, in consultation with their respective partners, as appropriate. Five agencies agreed with the recommendations, while four others neither agreed nor disagreed. Of the nine recommendations, three remain open.

- In August 2019, we identified that the Federal Energy Regulatory Commission's approved standards did not fully address NIST cybersecurity framework guidance for improving critical infrastructure cybersecurity.[8] We recommended that the Federal Energy Regulatory Commission consider our assessment and determine whether to direct the North American Electric Reliability Corporation to adopt any changes to its cybersecurity standards to ensure those standards more fully address the NIST cybersecurity framework and address current and projected risks. The Federal Energy Regulatory Commission agreed with our recommendation and planned to conduct a technical analysis and develop a plan to address it. Our recommendation to the Federal Energy Regulatory Commission remains open.
- In May 2020 we identified adverse impacts that varying cybersecurity requirements issued by four selected federal agencies had on state government agencies.[9] Each of four federal agencies had established cybersecurity requirements for states to follow in securing data. However, these requirements had conflicting parameters that involved agencies defining specific values. Examples of conflicting parameters included the number of consecutive unsuccessful logon attempts prior

[7]GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018).

[8]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

[9]GAO, *Cybersecurity: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States*, GAO-20-123 (Washington, D.C.: May 27, 2020).

to locking out users, the time to retain audit logs related to audited events, the frequency of security controls assessments, and the frequency of scans for system vulnerabilities. The percentage of total requirements with conflicting parameters ranged from 49 percent to 79 percent.

Our review found that state agency officials required to comply with multiple federal agencies' cybersecurity requirements (and related compliance assessments) viewed variances in these requirements as problematic and burdensome. Slightly more than half of state officials surveyed said that such requirements led to a great increase or very great increase in the time and staff hours needed to address the conflicts. We made 12 recommendations to agencies; eight of them are implemented and four are not, including two priority ones to the Office of Management and Budget to ensure agencies collaborate on requirements and state cybersecurity assessments.

- In September 2020 we reported about federal and nonfederal steps to enhance the security and resilience of the U.S. financial services sector.[10] However, we found that Treasury, as the designated lead agency for the financial sector, did not track efforts or prioritize them according to goals established by the sector. We made recommendations to Treasury to track and prioritize the sector's cyber risk mitigation efforts, and to update the sector's plan with metrics for measuring progress and information on how sector efforts will meet sector goals and requirements. While Treasury generally agreed with the recommendations, these recommendations remain open.

  Of note, selected financial firms identified the need for further assistance in improving harmonization among regulatory requirements. For example, four firms mentioned the difficulty of following differing state breach notification requirements, as compared to following one national requirement.

[10]GAO, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*, GAO-20-631 (Washington, D.C.: Sept. 17, 2020).

The Administration Initiated Actions to Harmonize Cybersecurity Regulations, but Significant Work Remains

Harmonization refers to the development and adoption of more consistent standards and regulations. Such consistency is important when critical infrastructure sectors are subject to multiple cybersecurity regulations. According to the White House, harmonizing regulatory requirements can lead to better security outcomes at lower costs.

To address this issue, the Administration and Congress have begun relevant initiatives to address the challenges associated with harmonizing cybersecurity regulations for our nation's critical infrastructure sectors. However, some of these actions are still underway and a planned completion date has not yet been announced.

As previously noted, in March 2023 and July 2023, respectively, the White House released the National Cybersecurity Strategy and the National Cybersecurity Strategy Implementation Plan.[11] Among other things, the strategy and implementation plan identified the need to establish an initiative on cybersecurity regulatory harmonization. As part of this initiative, ONCD was to engage with nongovernmental stakeholders through a request for information to understand existing challenges with regulatory overlap and explore a framework for reciprocity for baseline requirements.

In May 2024, the Administration issued its National Cybersecurity Strategy Implementation Plan (version 2), to update the previous year's version. Ongoing initiatives cited in the plan included setting minimum cybersecurity requirements across critical infrastructure sectors and increasing agency use of frameworks and international standards to inform regulatory alignment. In addition, the Administration added a new initiative to explore cybersecurity regulatory reciprocity pilot programs. The plan specifies that all of these initiatives will be completed by March 2025, or earlier.

In August 2023, in support of a National Cybersecurity Strategy strategic objective, ONCD issued a request for information that invited public

[11]The White House, *National Cybersecurity Strategy*, (Washington, D.C.: March 2023) and *National Cybersecurity Strategy Implementation Plan* (Washington, D.C.: July 2023).

comments on opportunities for, and obstacles to, harmonizing cybersecurity regulations.[12] ONCD stated that it was seeking input from stakeholders to understand existing challenges with regulatory overlap and explore a framework for reciprocity in regulator acceptance of other regulators' recognition of compliance with baseline requirements.[13] According to Regulations.gov, ONCD received over 100 comments on its request for information during the comment period, which closed in early November 2023.[14] ONCD has not published a summary of the comments.

Additionally, in April 2024, the Administration released National Security Memorandum-22, National Security Memorandum on Critical Infrastructure Security and Resilience.[15] Among other things, the memorandum calls for specific actions to be taken in support of the harmonization of cybersecurity regulations.

- Federal departments and agencies with regulatory authorities are to use regulation, drawing on existing consensus standards as appropriate, to establish minimum requirements and effective accountability mechanisms for the security and resilience of critical infrastructure.
- The National Cyber Director, in coordination with the Director of the Office of Management and Budget, is to lead the Administration's efforts for cybersecurity regulatory harmonization with respect to security and resilience requirements.
- The Secretary of Homeland Security is to develop and submit to the President by April 30, 2025, and on a recurring basis every 2 years thereafter by June 30, a National Infrastructure Risk Management Plan. The current National Infrastructure Protection Plan for securing critical infrastructure, which provides the overarching approach for integrating the nation's critical infrastructure protection and resilience

[12]Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations, 88 Fed. Reg. 55,694 (Aug. 16, 2023).

[13]ONCD defined reciprocity in this context as the recognition or acceptance by one regulatory agency of another agency's assessment, determination, finding, or conclusion with respect to the extent of a regulated entity's compliance with certain cybersecurity requirements.

[14]Regulations.gov is a website where the public can comment on proposed federal rules and regulations, See https://www.regulations.gov/document/ONCD-2023-0001-0001.

[15]The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience,* National Security Memorandum-22 (Washington, D.C.: Apr. 30, 2024).

activities into a single national effort, has not been updated since 2013.[16] Among other things, the updated National Infrastructure Risk Management Plan is to include:

- the identification, harmonization, and development of recommended national and cross-sector minimum security and resilience requirements to mitigate cross-sector risks not covered under sector-specific requirements; and
- a plan for harmonizing minimum security and resilience requirements across all sectors based on input from sector risk management agencies and other relevant federal departments and agencies.[17]

In addition, Congress and the President enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA was intended to help prioritize efforts to combat cyber threats by requiring certain entities to submit cyber incident reports to the Department of Homeland Security (DHS).[18] DHS's Cybersecurity and Infrastructure Security Agency (CISA) published a Notice of Proposed Rulemaking on April 4, 2024, seeking public comments on implementing CIRCIA's requirements, including ways to harmonize this regulation with other existing federal reporting requirements.[19] The deadline for comments is July 3, 2024.

CIRCIA also established a Cyber Incident Reporting Council (CIRC) to coordinate, deconflict, and harmonize federal incident reporting requirements, including those issued through regulation.[20] According to DHS, the Secretary of Homeland Security delegated responsibility to

[16]The Homeland Security Act of 2002, as amended, required DHS to develop a national plan for securing critical infrastructure and Presidential Policy Directive-21 required DHS to update that plan. See, 6 U.S.C. § 652(e)(1)(E) and The White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). As of April 2024, National Security Memorandum-22 superseded Presidential Policy Directive-21.

[17]Sector risk management agencies serve as day-to-day federal interfaces for their designated critical infrastructure sector and conduct sector-specific risk management and resilience activities.

[18]We have ongoing work related to DHS's efforts to implement the requirements of CIRCIA and plan to issue our report in the summer of 2024.

[19]Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644 (Apr. 4, 2024).

[20]Pub. L. No. 117-103, div. Y, sec. 103(a), 136 Stat. 49, 1054 (Mar. 15, 2022).

chair the CIRC to the DHS Under Secretary for Strategy, Policy, and Plans.

Further, CIRCIA required DHS to issue a report regarding cybersecurity regulatory harmonization. In response, in September 2023, the department issued its Harmonization of Cyber Incident Reporting to the Federal Government.[21] DHS invited the CIRC and 33 agencies to participate in developing the report to Congress. Among other things, the report identified 52 current or proposed federal cybersecurity incident reporting requirements, potentially duplicative federal reporting, and challenges to harmonization of these requirements. Such challenges include differences in the:

- definitions of reportable cyber incidents and thresholds for reporting,
- timelines and triggers for reporting,
- contents of incident reports,
- reporting mechanisms,
- procedural and resource burdens, and
- legal barriers and limited agency authorities.

The report also included eight recommendations that the federal government could adopt to streamline and harmonize cyber incident reporting, and three proposed legislative changes. For example, the report recommended that the federal government adopt model definitions of a reportable cyber incident, reporting timelines, and reporting triggers. The report also proposed that Congress remove any legal or statutory barriers to harmonization identified by the CIRC, including authorizing adoption of the model definitions of a reportable cyber incident, timeline, and trigger provisions.

As noted previously, although both the Administration and Congress have taken important initial steps on the issue of cybersecurity regulatory harmonization, significant work remains to be completed. Specifically, the Administration's efforts to evaluate setting minimum cybersecurity requirements across infrastructure sectors, increase agency use of frameworks and international standards to inform regulatory alignment, and leverage reciprocity pilot programs are still ongoing. In addition, DHS's September 2023 report noted that the CIRC would begin the

[21]DHS, *Harmonization of Cyber Incident Reporting to the Federal Government* (Washington, D.C.: Sept. 19, 2023).

process of implementing the report's recommendations, but did not provide a date for beginning the process or the completion of that work.

These key initial steps and their results can inform the broader effort and longer-term strategy to harmonize cybersecurity regulations, including future plans such as updates to the National Risk Management Plan. This underscores the importance of continuing to make progress on these key initiatives and continuing to address this significant issue.

In summary, as work continues on this important effort, it is vital that the stakeholders involved in this process remain focused on resolving the conflicts, inconsistencies, and redundancies currently found in our nation's cybersecurity regulations. Following through and executing specific plans and meeting established time frames, as supported by key organizations such as ONCD, DHS, and Congress, are essential to achieving harmonization. This, in turn, can better position our country's critical infrastructure sectors to address cybersecurity from a common perspective and help ensure the future safety and security of our nation.

Chairman Peters, Ranking Member Paul, and Members of the Committee, this completes my prepared statement. I would be pleased to respond to any questions that you might have.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact David B. Hinchman, Director of Information Technology and Cybersecurity, at (214) 777-5719, hinchmand@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Michael Gilmore (Assistant Director), Josh Leiling (Assistant Director), Kavita Daitnarayan (Analyst-in-Charge), Amanda Andrade, Tracey Bass, Alexander Engel, Rebecca Eyler, Dwayne Staten, and Scott Pettis.

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 Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or 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 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Sarah Kaczmarek, Acting Managing Director, KaczmarekS@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548