TLP:CLEAR

Cyber Storm IX: After-Action Report

September 2024
Cybersecurity and Infrastructure Security Agency (CISA)

TLP:CLEAR

TABLE OF CONTENTS

Executive Summary 1
Key Achievements 2
Exercise Overview 3
Exercise Goal & Objectives 4
Participation 4
Scenario & Adversary 4
Exercise Findings 5
Finding 1: Cloud Security 5
Finding 2: Internal Processes 8
Finding 3: Facilitating Information Sharing 10
Finding 4: Incident Reporting 13
Finding 5: Federal Coordination 16
Finding 6: International Coordination 18
Finding 7: Distributed Information Sharing Networks 19
Finding 8: Established Relationships 21
Consolidated Cyber Storm IX recommendations 23
Cybersecurity Documents Referenced in the After-Action Report 26
List of Acronyms 27
Appendix A: Participant List 29
Appendix B: Exercise Design Summary 34

EXECUTIVE SUMMARY

Cybersecurity has become an essential capability, protecting our information systems and, by extension, operation of the critical infrastructure upon which our way of life depends. To face an evolving threat landscape, we require a robust national cybersecurity posture that enhances cyber preparedness, response capabilities, and cross-sector coordination for critical infrastructure operators and government partners alike. Since 2006, the Cyber Storm exercise series, sponsored by the Cybersecurity and Infrastructure Security Agency (CISA), has provided a venue for stakeholders to exercise cybersecurity processes together, strengthening the collective resilience of critical infrastructure.

Since the publication of the National Cybersecurity Strategy (NCS) in 2023, an array of national reports and studies have signaled that the federal government is engaged in an ongoing process to reassess federal and partner responsibilities for safeguarding the nation's critical infrastructure. With hundreds of United States (U.S.) public and private sector organizations participating alongside international partners, the Cyber Storm series is well-placed to exercise and evaluate current and future guidance.

Cyber Storm IX, held in April 2024, allowed over 2,200 participants from federal departments and agencies, state governments, critical infrastructure, and international partners to exercise incident response, information sharing, and coordination in response to a cyber campaign against U.S. and partners' critical infrastructure. The scenario explored cybersecurity vulnerabilities arising from improper configuration of cloud resources. Using the confidentiality, integrity, and availability triad as a framework, the exercise encouraged stakeholders to consider how an attack targeting these configurations could access data in the cloud. While multiple critical infrastructure sectors participated in the exercise, the Food and Agriculture Sector served as the primary impacted sector.

The Cyber Storm IX After-Action Report details the findings identified over the exercise lifecycle. These findings are derived from discoveries made during design and development, observations made during the exercise, and feedback documented in after-action questionnaires and at post-exercise evaluation events. The first finding relates to the technical scenario, while the remaining findings are intended to inform CISA and stakeholder improvement activities and have broad applicability to cyber incident response:

- **Finding 1:** Collective capabilities and shared responsibilities will help ensure cloud security remains resilient;
- **Finding 2:** As incident response planning matures, organizations continue to identify points of failure and challenges linking technical and business response;
- **Finding 3:** Stakeholders could be incentivized to provide more timely reporting of cyberattacks if the federal government facilitated broader, faster information sharing;
- **Finding 4:** The cybersecurity community desires streamlined federal incident reporting structures;
- **Finding 5:** Federal mechanisms for coordination during significant cyber incidents, as defined in national plans and policies, are not well understood;
- **Finding 6:** Processes for cyber information sharing between international partners need to mature further;
- **Finding 7:** Stakeholders value the timeliness and familiarity of distributed cyber information sharing networks and believe more could be done to improve their utility; and
- **Finding 8:** In a highly technical and automated field, established relationships are key to effective coordination.

Key Achievements

Cyber Storm IX built upon preceding iterations of the series to provide a venue for learning and advancement. Through the exercise planning process and execution, Cyber Storm IX:

- Strengthened cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a significant cyber incident impacting multiple critical infrastructure sectors;
- Provided participants the opportunity to stress a whole-of-organization response to an incident involving organizations' technical experts, public affairs representatives, legal affairs representatives, and organizational leadership;
- Engaged participating organizations' senior leadership in decision-making, encouraging them to consider how incident response plans and processes align to strategic priorities and governance principles;
- Validated the efforts many organizations have invested in building cloud incident response capabilities and procedures;
- Integrated a simulated and dynamically updated traditional and social media platform to replicate the customer and "general public" components of an incident and provided a no-fault learning environment to practice strategies that support comprehensive response;
- Exercised federal coordination procedures during a significant cyber incident, including a joint National Cyber Incident Scoring System (NCISS) assessment, federal Cyber Response Group (CRG) coordination, notional activation of a Cyber Unified Coordination Group (UCG), and enhanced coordination between key federal lines of effort during a significant cyber incident;
- Allowed participating states to closely examine the associated roles and responsibilities of supporting agencies within their cyber incident response frameworks and their relationship to federal response partners;
- Reinforced information sharing and communication processes between international partner nations; and
- Focused on a previously under-emphasized critical infrastructure sector, Food and Agriculture, and welcomed new stakeholders to Cyber Storm, supporting relationship-building and providing a foundation for future coordination and improvement efforts.

EXERCISE OVERVIEW

Sponsored by the Cybersecurity and Infrastructure Security Agency (CISA), Cyber Storm is CISA's biennial capstone exercise and is congressionally authorized as the National Cyber Exercise under the National Defense Authorization Act for Fiscal Year 2021. It is the most extensive government-sponsored cybersecurity exercise of its kind and offers a rare opportunity for the federal government, state governments, the private sector, and international partner nations to come together and exercise cyber response as a whole community. Starting with Cyber Storm I in 2006, the exercise has brought together stakeholders to assess and strengthen cyber preparedness by examining incident response processes. Cyber Storm IX built on this legacy, bringing public and private sector peers together to build new relationships, strengthen existing ones, and safeguard the nation's critical infrastructure by identifying best practices to strengthen coordinated incident response along the whole-of-nation approach outlined in the National Cyber Incident Response Plan (NCIRP).[1]

As an operations-based, functional exercise, Cyber Storm IX allowed players from participating organizations to simulate their response to a multi-sector significant cyber incident. The exercise evaluated incident response plans, processes, and procedures; coordination and information sharing capabilities; and governmental lines of effort while identifying opportunities for improvement. While players worked to resolve the cyberattacks targeting their own organizations, they also exercised their capacity to share information and coordinate incident response externally as part of a greater national effort.

The Cyber Storm exercise series has evolved over time in step with the changing cyber threat landscape and the maturation of national cyber incident coordination processes and industry best practices. The Cyber Storm IX scenario turned participating organizations' attention to risks associated with the misconfiguration of cloud services and to the compounding dangers of malicious user authentication and privilege escalation. Currently, federal policies for coordination in response to cyber incidents are undergoing reassessment. Cyber Storm IX was positioned to evaluate current strengths and areas for improvement in this area, specifically focusing on federal coordination processes and the "centralized" versus "federated" models for information sharing and incident reporting by impacted entities to the federal government during cyber incidents.[2]

In keeping with past iterations of the exercise that focused on a "sector of interest," Cyber Storm IX concentrated on the Food and Agriculture Sector. This focus was demonstrated by robust representation from the sector in the exercise including 30 private sector organizations, the Food and Agriculture Information Sharing and Analysis Center, and both relevant sector risk management agencies (SRMA): the U.S. Department of Agriculture and the Food and Drug Administration.

The Cyber Storm IX capstone exercise occurred in April 2024. Exercise players participated from their work locations across the globe while the exercise control cell managed overall play from CISA headquarters in Arlington, Virginia. More than 200 organizations participated over three days of play. In addition to the capstone exercise, the Cyber Storm IX program hosted six ancillary events during the exercise cycle: three seminars with states, two tabletop exercises with key public and private sector partners, and one tabletop exercise with members of the Food and Agriculture Sector. CISA held these events to introduce participating entities to cyber exercise principles, to review incident response best practices and federal guidance around coordination, and to prepare entities for participation in the Cyber Storm capstone.

[1] First published in 2016 and serving as the nation's framework for coordinated incident response to a significant cyber incident, the National Cyber Strategy directed that CISA update the NCIRP to "strengthen processes, procedures, and systems to more fully realize the policy that 'a call to one is a call to all.'" A draft version of NCIRP 2024 will soon be released for public comment.

[2] U.S. Government Accountability Office. "Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods," GAO-23-105468. September 26, 2023.

Exercise Goal & Objectives

Goal: Strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector significant cyber incident impacting critical infrastructure.

Objective 1: Exercise and evaluate cybersecurity response, operational collaboration, and support.
Objective 2: Examine and clarify roles and responsibilities in response to a significant cyber event.
Objective 3: Assess information sharing capabilities and resource needs during a cyber incident.
Objective 4: Review and evaluate relevant national cybersecurity policy, guidance, and doctrine.

Participation

Cyber Storm IX included participants from federal, state, and private sector organizations, as well as international partners.

- More than 100 private sector organizations spanned 12 critical infrastructure sectors.
- 35 federal departments and agencies included organizations responsible for threat response, asset response, intelligence support, private sector coordination, and public services.
- 13 participating and/or observing states included components of law enforcement, administrative, and public-service organizations.
- 11 partner nations joined the U.S. in exercising their information sharing and incident response coordination.
- Within organizations, Cyber Storm IX players spanned from operational shop floor and front-line customer care staff to security and technical responders, incident response teams, legal affairs specialists, public affairs specialists, and senior leaders.

Scenario & Adversary

As more companies in the U.S. seek solutions for cost efficiency, reliability, and flexibility, they have turned to cloud service providers (CSP) for everything from applications, or software as a service, to virtualized networks and hardware, or infrastructure as a service. The exercise tested the level of customer/stakeholder knowledge of the specifics of the shared responsibility model for cloud security. The core scenario for Cyber Storm IX was split into two broad vulnerabilities that resulted from either misapplying the shared responsibility model of cloud security or not implementing industry best practices. The first vulnerability leveraged poor software development lifecycle processes, while the second vulnerability arose from poor identity access management practices when using the cloud, which allowed attackers to exploit this access for their own purposes. To disrupt critical infrastructure in the U.S. and among partner nations, a fictitious adversary group named the NS9 Snakes developed a rootkit, ADAMWare. This fictional rootkit allowed attackers to gain access to customer cloud environments and perform multiple attacks simultaneously. These attacks included lateral movement, privilege escalation, share enumeration and file harvesting, and full administrator-level access to environments.

As a result of heightened security measures, open internet-facing applications are not prevalent in some organizations. In these instances, the attackers modified the code to allow for social engineered delivery. Some organizations received phishing emails while others fell victim to watering hole attacks. In all instances, the

adversaries exploited the attack vector to connect to the initial command and control or staging server, execute commands, and then employ known tools (e.g., Cobalt Strike). This rootkit was developed from multiple common vulnerabilities and exposures found in the Shadow Brokers release from 2016. However, ADAMWare had modified code and its rootkit contained previously undisclosed exploits.

EXERCISE FINDINGS

Organizations participating in Cyber Storm IX tested their incident response policies and procedures to identify gaps and areas for improvement, both for internal response and in coordination with external partners. This report incorporates experiences and feedback from across the federal government, state governments, coordination bodies, the private sector, and the international community. Data was gathered from observations recorded during the exercise, participant questionnaires, stakeholder debriefs, and comments gathered at post-exercise evaluation events including the exercise hotwash and the after-action meeting. The following section contains eight exercise findings, supported by observations drawn from exercise play. Each finding is followed by a list of recommendations offered by participants intended to address these findings and strengthen the nation's coordinated response to cyber incidents.

Finding 1: Collective capabilities and shared responsibilities across stakeholders will ensure that cloud security remains resilient.

The migration from on-premises solutions to cloud-based solutions offers customers improvements in flexibility, scalability, cost efficiency, reliability, and security. Cyber Storm IX found that maturity around cloud security issues varied among security and incident response personnel in both the public and private sectors. This gap presents a target of opportunity to adversaries seeking to exploit vulnerabilities across critical infrastructure.

> "Our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations and individual citizens. Instead, across both the public and private sectors, we must ask more of the most capable and best-positioned actors to make our digital ecosystem secure and resilient. In a free and interconnected society, protecting data and assuring the reliability of critical systems must be the responsibility of the owners and operators of the systems that hold our data and make our society function, as well as of the technology providers that build and service these systems."
>
> - National Cybersecurity Strategy, March 2023

Customers and cloud service providers' understandings of responsibility are misaligned.

The Cyber Storm IX scenario examined cloud credentialing and privileged access in customer environments, prompting stakeholders to examine their organization's identity-management practices and consider which security settings are within their control. Exercise play revealed that customer maturity, in terms of familiarity with the security of their cloud environments, varied widely and that some customers' understanding of roles and responsibilities under the shared responsibility model is relatively immature. Many customers were surprised that during an incident, CSPs have limited insights into the unique characteristics, contents, or potential exposure of a customer's workload or data.

In the cloud computing model, security responsibilities are shared between the CSP and the customer. CSPs establish the cloud infrastructure, providing a ready-to-operate environment for the customer and provide secure-by-default configurations to ensure customers start from a high security baseline. CSPs intentionally design their services for the highest levels of privacy and security, meaning they do not have access or visibility

into their customers' workloads. During an incident, CSPs have limited insights into the unique characteristics, contents, or potential exposure of a customer's workload or data. Therefore, the customer bears responsibility for detecting and responding to incidents within their cloud environments, without relying extensively on CSP involvement or visibility into their workloads. Because of this, it is incumbent on the customer to develop a secure-by-design architecture prior to development or production in the cloud. Securing the cloud is contingent on both parties' understanding of this model.

> "We were familiar with our CSP and their platform going into the exercise, but there's still a fundamental need to increase our knowledge… Before migration or development in the cloud, we have a number of requirements that have to be baked into the design and we do a security assessment before any application come to production…There's a shared responsibility and I agree that we have a responsibility for a minimum requirement, but CSPs need to leverage their expertise to provide more guidance." - Cyber Storm IX participant

While this may be reflective of the current state, a report from the federal Cyber Safety Review Board (CSRB) addressing a specific cloud-based identity access management incident has laid out a number of best practices to establish common baselines for cloud security.[3] Some CSPs have drawn criticism for failing to provide customers with basic security logging capabilities to detect and respond to cyber threats in their environment, absent purchase of premium enterprise product bundles. It is the hope that these best practices, many of which are already implemented by industry leading CSPs, will be implemented industry wide. Exercise participants suggested that the relative lack of digital identity standards is an ecosystem-wide issue, requiring investment by industry and government.

Specific to identity management, CSPs stated that customers' responsibility for identity management including keys, certificates, passwords, single sign-on, and multi-factor authentication, depends on which cloud services the customer uses and how it has configured the CSP's services. For example, some customers manage their own keys while others use key managed services provided by CSPs. However, the CSRB has found "that the current ecosystem of digital identity standards does not provide the security necessary to counter modern threat actors, and that some CSPs have not sufficiently prioritized implementing emerging standards that improve the security of digital identity systems."[4]

Fundamentally, customers and CSPs view cloud security as a collaborative challenge that must be overcome via general implementation of best practices, improved access to security tools, and continued education on responsibilities, capabilities, and resources. While customers, as the users and owners of the data, acknowledge their responsibility for the risk, CSPs are the most knowledgeable and experienced actors about their solutions and should continue to provide customers with security best practices and the appropriate tools to ensure their data remains protected in the cloud. At the same time, customers have a responsibility to implement the tools provided by the CSPs. CSPs operating under a "shared fate" model recognize the misalignments that can occur from limited CSP visibility into customer workloads and the limited cloud expertise of customers. To address this, they provide resources, training, secure-by-default architecture blueprints, secure configuration guidance, and other support to help customers understand CSP limitations, their own responsibilities and the skills to manage their environments securely.

Participating customer incident response teams lack familiarity with CSP capabilities or engagement processes.

During a cybersecurity incident affecting data in the cloud, impacted customers can engage with their CSP. While the degree of support the CSP offers may be limited by the customer's architecture and by the service level

[3] Cyber Safety Review Board. Review of the Summer 2023 Microsoft Exchange Online Intrusion. March 20, 2024.
[4] *Ibid*, p. 22.

agreement (SLA), the CSP can offer insight on log transactions, impacts to the environment, and considerations related to recovery and restoration. To model this, CSP personnel staffed the Simulation Cell (SimCell) to assist customers with investigation and response to the simulated cyberattack as it unfolded during the exercise. During the exercise, CSPs received considerably fewer inquiries than anticipated. Inquiries they did receive focused on account lockouts, data loss, and network connectivity issues.

Acknowledging that the exercise cannot completely replicate real-world coordination between customers and CSPs and that not all organizations had reached "discovery" of a cloud-related incident by the end of the exercise, the data suggests impacted organizations are not quick to engage with their CSP during a cyber incident that affects their cloud resources. Many organizations had invested in building cloud incident response capabilities and procedures, and in turn may not have had a need to engage with CSPs in the SimCell for assistance.

Adding complexity to this challenge, many organizations also procure and manage their cloud services through resellers or managed service providers (MSPs). Organizations participating in the exercise noted they did not have direct contacts at major CSPs but instead work through other vendors or contractors. Using a reseller or MSP introduces an additional layer of complexity for coordination and communication efforts, as organizations would typically contact their reseller or MSP and not the CSP. At the same time, MSPs and resellers may have significant knowledge of CSP capabilities, security features and engagement procedures, making resellers and MSPs an important and efficient source of key information for customers during an incident.

CSPs perform their information-sharing responsibilities during widespread incidents.

CSPs play an important role in information-sharing as providers of threat intelligence to their customers. In addition, CSPs adhere to legal requirements for incident reporting set forth by the federal government but are protected from disclosing activities that would identify or endanger customers as public sharing could signal to an adversary that impacted organizations are aware of an intrusion. Furthermore, CSPs do not have visibility into a customer's workload and therefore cannot discover all intrusions. Where appropriate, CSPs alert customers proactively of widespread campaigns or vulnerabilities such as Log4j. As the CSRB articulated, customers and the federal government look to CSPs to continue sharing information with federal partners and with impacted or threatened entities and to prioritize this information sharing over other business considerations.[5]

Customers are insufficiently familiar with SLAs and CSP restoration processes.

A common theme throughout exercise planning and conduct was that customers' incident response staff are typically unfamiliar with the contractual limitations defined in their SLAs with CSPs. Organizations need to be familiar with these SLAs to have a realistic understanding of their CSP's response capabilities, obligations, and timeline during an incident. Prior to the exercise, most participants had not examined their SLAs in depth and identified a need to do so following the exercise. Organizations should review their SLAs and update their plans following any major changes to account for projected incident response limitations.

Multiple organizations noted that the exercise revealed gaps in their understanding of how SLAs can affect the account restoration process such as the timeframe involved and the documentation required for account access recovery and validation. In their interactions with the SimCell, organizations gained a better understanding of the "break glass" process used to bypass normal security controls to regain access to an account.

Customers require ongoing CSP-provided training.

Although it is the customer's responsibility to configure security for their workloads hosted in the cloud, organizations benefit from guidance from their CSP on cloud security best practices, a better understanding of assistance the CSP can provide during an incident, and a clear grasp of the difference between the CSP's and customer's responsibilities. Cyber Storm IX validated that CSPs do play a role in incident response and customers

[5] Cyber Safety Review Board. Review of the Summer 2023 Microsoft Exchange Online Intrusion. March 20, 2024, p. 22.

would benefit from additional engagement around this topic.

Post-exercise feedback from planners and players highlighted the need to improve staff education and training on cloud security tools. CSPs take the responsibility to advise organizations seriously and offer significant materials, trainings, and tools to improve customer understanding. The challenge is making materials and training available to the appropriate staff in a customer organization—a challenge customers have a role in resolving. During exercise play, the Cloud Security Alliance recognized (in a simulated exercise press release) that "organizations have different maturity levels for their security programs and may be challenged to find skilled staff critical to the development and implementation of a zero-trust strategy," which is a cloud security best practice. With many incident response plans geared toward on-premises resources, Cyber Storm IX was an impetus for organizations to update their plans and acknowledge the nuances and responsibilities to secure their cloud resources.

Stakeholder-Derived Recommendations:

- Cloud customers should continuously monitor their cloud security configurations and controls and conduct a thorough assessment of their auditing, logging, identity management, and recovery processes.
- Cloud customers should enact strong security practices (e.g., zero-trust models, key rotation, principle of least privilege) surrounding the creation, use, and monitoring of administrative cloud credentials to maintain the integrity, confidentiality, and availability of cloud-based systems and data.
- Cloud customers should enhance their security baseline using tools such as the Center for Internet Security (CIS) benchmark program and should prioritize training staff on cloud security.
- Cloud customers should examine their SLA and work with their CSP to ensure they have the necessary level of service and support in the event of an incident.
- CSPs should provide guidance to customers on secure-by-default blueprints and landing zones, provide security enhancements, and proactively inform customers about risks related to their configurations.
- CSPs should educate customers on the limitations of CSP visibility and access into customers workloads in the event of an incident so they can adjust incident response plans accordingly.
- CISA should continue to provide Secure by Design guidance and collaborate with CSPs to make security configurations widely available regardless of license tier as they did with the expanded logging capabilities announced in CISA's Press Release on February 21, 2024.
- Cloud customers should reference the CSA's Cloud Incident Response Framework when incorporating the shared responsibility model into their incident response plans.
- Cloud stakeholders should continue to look to the Federal Risk and Authorization Management Program, a key governance program for the federal government and an influential standard for other sectors, which helps ensure stronger cybersecurity practices, including in cloud-based digital identity, across the cloud service ecosystem.

Finding 2: As incident response planning matures, organizations continue to identify points of failure and challenges linking technical and business response.

During the exercise, organizations in every sector grappled with the challenge of single points of failure including inexperience of new staff at critical points (e.g., help desk), the absence of experienced incident commanders/executive decision makers, or the absence of system experts. Many organizations also continue to work on linking their technical response to other business functions during an incident. Participants identified

two categories of challenge, around timing for engagement with legal counsel, public information, and business leadership and identifying the right information to communicate to them.

Internal communication methods must be up to date and resilient.

The exercise shed light on the potential communication issues that could affect transmission of important information during an incident. During the exercise, some organizations found they did not have set processes internally for who to contact, when to contact them, and what information is appropriate to share. Some organizations found their prescribed communication methods were not optimal for incident response. Additionally, some organizations discovered that during an incident, their primary method of communication was inoperable and they did not have a secondary method on record, making coordination difficult and time-consuming. To address this, it is imperative that effective information-sharing channels are in place prior to a real-world incident, the appropriate personnel for incident response are known, and backup methods of communication are established in case primary methods cannot be used during an incident.

Several organizations—in particular, larger critical infrastructure entities and state governments—identified a need for a consolidated, "out of band" communications tool that can be used during a cyber incident. This channel can function as a common information-sharing space where stakeholders from across the organization can collaborate. This helps to prevent siloing of workstreams and information that may be relevant to multiple teams. Participants mentioned several options, including Slack and the Homeland Security Information Network; these tools can also double as channels for cyber awareness, facilitating threat intelligence sharing and acclimating users to the channel as a cyber incident coordination tool.

Identifying the correct time for external information sharing is an internal decision.

External information sharing is an important part of effective incident response, but many participants had trouble identifying external points of contact during an incident. When dealing with an ongoing incident, organizations noted it is challenging to identify the appropriate points of contact at other organizations, meaning that external coordination does not always occur. The delay in or absence of external coordination can jeopardize effective response. Proactive planning, to include establishing a matrix of who to contact and when, ensures an avenue for collaboration during a real-world incident. Cyber Storm IX allowed participating organizations to work together and become more comfortable with the process of collaboration outside their own organization. Additionally, participants highlighted that being aware of other organizations' processes and incidents aided their own incident responses. These organizations were able to adjust their own responses in accordance with the larger scenario, which they would not have been able to do had they not collaborated with each other.

Appropriate roles and responsibilities help effectively manage an incident.

Throughout the exercise, organizations found that having the correct staffing and internal training is key to incident response. Organizations found that the teams within the exercise who had previously established clear roles and responsibilities had an easier time dealing with an incident. Many organizations found that during the exercise, they were not familiar with who they should contact regarding an incident, which led to confusion and critical lost time. Organizations also found there were gaps in expertise. These organizations discovered they did not have the appropriate personnel to deal with an incident or experienced personnel to fill those gaps. Organizations confirmed incident response plans need to clearly align roles with responsibilities prior to an incident so that when dealing with a real-world issue, their staff would be aware of the management chains and incident response teams they should contact.

Additionally, organizations highlighted the need for more internal training regarding their incident response procedures. They discovered that even if they had the correctly defined roles during an incident, more effective training for staff prior to the incident would have aided the organization's incident response. Beneficial trainings identified in the exercise include technical training for cloud system owners and operators, media training for

those responding to public information queries, trainings specifically tailored to leadership, and general cyber incident response training.

Organizations can strengthen their preparedness by reviewing and updating plans.

Most organizations model their incident response plans on the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. During the exercise, organizations evaluating their plans discovered they needed to be updated with insights from the exercise. These insights chiefly related to internal communication, external communication with CSPs and MSPs, and engagement with information-sharing partners, including ISACs and federal departments and agencies. Organizations should update these documents and ensure staff are trained on the plans prior to an incident. Participants recommended that plans should present a holistic view for all stakeholders while also including checklists for specific roles.

Many organizations discovered their plans had gaps for responding to a cyber incident, and that updated, templated documentation would have saved time, energy, and business operations within their organization. Participants recommended appropriate documentation should clearly lay out internal and external roles and responsibilities, establish guidelines for appropriate information sharing, and describe incident response processes and the resources associated with these processes.

Stakeholder-Derived Recommendations:

- Organizations should review incident response plans to ensure roles and responsibilities are clearly defined and to minimize individual points of failure.
- Organizations should establish, document, exercise, and educate staff on incident response communication channels prior to an attack.
- Organizations should develop a primary, alternate, contingency, emergency (PACE) plan that identifies backup methods of communication.
- Organizations' incident response plans should incorporate a list of external collaborators including capabilities, points of contact, and thresholds for coordination.
- Organizations should review or exercise processes for engaging MSPs prior to an incident and establish processes where they do not exist.

Finding 3: Stakeholders could be incentivized to provide more timely reporting of cyber incidents if the federal government facilitated broader, faster information sharing.

Stakeholders agreed that effective cybersecurity hinges on timely and accurate reporting of cyber incidents. Cyber Storm IX explored and identified several ways to optimize federal reporting, including streamlining processes, enhancing reporting incentives, addressing concerns about confidentiality, and implementing increased feedback post-reporting. These improvements would strengthen federal reporting and thereby bolster collective defense against cyber threats.

The federal government should streamline information sharing processes to make threat information more accessible.

Participants value the threat intelligence that the federal government shares but are frustrated by the real-world artificial barriers that choke the flow of relevant information to impacted or threatened organizations. The September 2023 U.S. Government Accountability Office (GAO) report on information sharing performance measures and methods found that limited sharing of classified or sensitive information is a challenge to effective information sharing. This review of 14 federal and 7 nonfederal agencies identified factors that facilitate and

challenge cyber threat information sharing; 13 of the 21 entities reported that limited sharing of classified or sensitive information was a challenge to cyber threat information sharing.[6] During the exercise, critical infrastructure and state government partners cited their frustration in three areas:

- Numerous personnel at critical infrastructure and state government entities have been vetted for public trust or hold security clearances, yet federal partners do not share sensitive or classified information with them due to what these partners perceive as a lack of trust. While participants acknowledged that there may be logistical obstacles to the sharing of information, including access to classified systems or spaces, they felt that fundamentally, the lack of federal sharing stemmed either from an assumption that personnel outside the federal government were not appropriately vetted or should not be privy to sensitive or classified information, or that personnel outside the federal government could not be trusted to respect sensitivity designations and would share information with other individuals who had not been similarly vetted.
- Related to the last point, participants reported recurring uncertainty about what information could be shared with other organizations and when. ISACs expressed frustration that sometimes they would receive sensitive information from one member, share it with federal partners, and then be asked by the federal government not to share it with other members. More ambiguously, ISACs would also sometimes receive threat intelligence from the federal government without clear indication of what they could share with their members. Other organizations with information sharing relationships, including state governments, shared similar experiences.
- During Cyber Storm IX, participants across the exercise, including federal partners and members of the intelligence community, concurred that deliberation on information sharing sensitivities like appropriate Traffic Light Protocol (TLP) designation was unnecessarily drawn out and that much of what was deemed sensitive (due to perceived importance) was open-source or private sector-provided information and therefore did not require a rigorous vetting process.

Counterbalancing the desire for faster and more detailed information sharing is a recognized need to protect the confidentiality of information shared by impacted entities. Participants agreed that rigorous processes to protect the privacy of impacted organizations and their sensitive information should be formalized. However, they suggested that once information has been sanitized, it should be made generally available to the vetted cybersecurity community. Some participants suggested this could be accomplished with the creation of a general threat information database populated with indicators of compromise (IOC), tactics, techniques, and procedures (TTP), and other threat intelligence—in essence, an evolution of CISA's Known Exploited Vulnerabilities Catalog. Participants acknowledged that there might be classification challenges if threat intelligence was derived from intelligence community sources but suggested that the database could have different tiers of access or that more sensitive information could be kept behind an access wall unless a senior leader (such as the Secretary of Homeland Security, National Cyber Director, or Director of CISA) designated dissemination to a larger access group in response to an imminent threat.

Fundamentally, to support broader information sharing the federal government must streamline its information sharing processes. Participants recognize that different segments of the cybersecurity community, including the federal government and customers of their threat information, have their own equities and priorities and therefore approach this problem differently. But whether the federal government addresses this challenge by designating open-source information to have a lower sensitivity, engaging vetted stakeholders more proactively, broadening the network of vetted stakeholders, centralizing threat information in a single repository, or simply formalizing, clarifying, and optimizing the processes around information sensitivity, sanitizing, and sharing, it is

[6] U.S. Government Accountability Office. "Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods," GAO-23-105468. September 26, 2023.

clear this is a major friction point that must be addressed.

Organizations are not incentivized to report cyber incidents.

Mandatory incident reporting has an incentive problem. In the current environment, there are neither clear rewards for meeting reporting guidelines nor penalties for failing to do so. Stakeholders do not understand how they will benefit from sharing information with the federal government. Furthermore, stakeholders can face internal restrictions imposed by leadership and legal counsels designed to limit reputational damage and legal liability that would stem from admission of the incident. Simply put, without clear incentives, stakeholders are not motivated to report.

Stakeholders stressed the need for timely and informative follow-up on reported incidents. In the exercise, players did not receive follow-up after reporting an incident. Without a clear understanding of next steps in the reporting process, stakeholders are unmotivated to report in the future, uncertain how reporting would benefit them. CISA should include a feedback stage in the reporting process for entities reporting incidents to provide regular updates. This implementation would result in broader situational awareness, leading to faster reporting, response, and recovery. By fostering a more collaborative and equally informed process, stakeholders will be more involved in the reporting process and, therefore, be more likely to report an incident when it occurs.

Participants suggested that the federal government could build trust by first engaging stakeholders via an ISAC, fusion center, or other means, when it becomes aware of an incident. During the exercise, some impacted entities reported they would be more likely to report information during an incident if there was two-way communication with the federal government. Stakeholders felt that during the exercise, federal agencies were not proactive in following up with victim entities to understand the nature of the impact. Direct federal engagement via federal cyber centers, agency regional and field offices, or SRMAs would open the lines of communication, thereby promoting incident reporting from impacted entities. In fact, CISA has introduced a process for two-way tactical coordination in the early stages of an emerging incident via the Joint Cyber Defense Collaborative (JCDC), which presents one path forward for improving timely, valuable operational collaboration between public and private sector partners.

Organizations are concerned about confidentiality and liability.

The challenge with broader information sharing is safeguarding the confidentiality of sensitive information. Participants noted the difficulty of determining the appropriate level of detail to include in reports and the pitfalls of sharing incomplete or incorrect information. Concerned about security risks and legal liability, organizations need to understand how their information will be used. Developing clear guidelines and legal understanding for information sharing could help alleviate these concerns and facilitate faster and broader information sharing.

Exercise participants expressed concerns about confidentiality and liability. They called for increased transparency from CISA regarding reporting processes and handling of sensitive data. The absence of anonymous reporting channels or guidelines for confidential reporting contribute to hesitation in sharing information. Stakeholders emphasized the importance of knowing how their data will be used and how their sensitive information will be protected. Improving transparency and communication could enhance trust and confidence among stakeholders, encouraging them to share information more readily.

Stakeholder-Derived Recommendations:

- The federal government should review parameters and processes for vetting cybersecurity partners and prioritize optimal use of those information sharing relationships.
- The federal government should simplify sensitivity designation and handling instructions for shared information while aligning to TLP guidance.
- The federal government should review incident report sanitization processes to ensure they are airtight and streamlined to safeguard the reporting entity's anonymity while generating threat information that can be shared with a larger community of stakeholders.
- To ensure the timely sharing of TTPs and IOCs, the federal government should share on a rolling basis rather than waiting to prepare a full-length report.
- The federal government should continue development and publicization of the Known Exploited Vulnerabilities Catalog as the primary federal repository for up-to-date threat information.
- To overcome institutional barriers to incident reporting, the federal government should drive faster, more detailed, and more frequent incident reporting by developing a standard process to acknowledge reporting, provide value to impacted entities, and educate impacted entities on the protections they can expect.

Finding 4: The cybersecurity community desires streamlined federal incident reporting structures.

Despite best intentions, stakeholders have expressed frustration with the expanding and often redundant guidelines for cyber incident reporting to different federal departments and agencies. Currently, an entity that suffers a cyber incident may submit similar reports to multiple federal agencies via multiple mechanisms and systems, leading to duplicative efforts on the part of the reporting entity. Specifically, entities including SRMAs, CISA, the FBI, and other information-sharing bodies such as ISACs are all part of the incident reporting ecosystem. This federated incident reporting model creates additional effort for the reporting organization. It requires them to report the same information to multiple agencies, creating confusion about which specific entity to report to at a given stage of the incident response process. It is unclear what intelligence or response capabilities the impacted entity will receive from that agency in exchange.

During the exercise, organizations reported they would be more likely to report an incident to the federal government, and do so more promptly and in greater detail, if reporting channels are clearly defined and easily navigated. Having a consolidated incident reporting structure, with one agency as the primary point of contact, will streamline the reporting process for impacted organizations. Given the role that the NCIRP designates to CISA as the primary agency for asset response during a significant cyber incident, along with its existing authorities, capabilities and maturing relationships, organizations reported that CISA is the logical lead agency for a consolidated incident reporting structure.[7]

[7] Cyber Storm IX is intended to strengthen cybersecurity and response capabilities by exercising policies, processes, and procedures that are currently in effect in order to replicate a real-world experience. For this reason, the Cyber Storm IX exercise did not include reporting requirements or legal authorities that were not in effect, such as regulatory reporting requirements that will be implemented through the rulemaking process for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Cyber Storm IX exercise participants were directed by CISA staff to submit all feedback on the CIRCIA rulemaking through www.regulations.gov in order for their comments to be considered by CISA as part of the rulemaking process for the final rule.

A consolidated incident reporting structure can reduce burdens on impacted organizations and facilitate broader sharing of information to the federal government.

> "The federal government should minimize the burden on the private sector to report the same or similar information through multiple channels, and the federal government should bear the burden to 'connect the dots' and disseminate information to multiple federal agencies with legitimate need to receive the information reported. A common reporting platform and intra-government information sharing infrastructure will be increasingly necessary to alleviate the burden of duplicative reporting."
>
> - DHS Office of Strategy, Policy, and Plans (OSPP), Harmonization of Cyber Incident Reporting to the Federal Government, 2023

During the exercise, some participating organizations reported that the distributed incident reporting structure constrained the ability to report incident details to the federal government in an efficient manner. For example, in the event of a cyber incident that affects a state government, reporting requirements to SRMAs covering each state agency can quickly become arduous. An impacted state may have to report to multiple federal agencies if multiple state agencies are impacted. For instance, a state would have to report to the Department of the Treasury if their state department of taxation is impacted, the Department of Health and Human Services if there are impacts to the state health agency, or Department of Homeland Security (DHS) and the Department of Transportation if there are impacts to state transportation infrastructure. A consolidated incident reporting structure, where impacted entities can report to one portal or network and information is subsequently dispersed to appropriate agencies, would allow information to be shared efficiently while eliminating duplicative processes.

Having a lead agency that serves as the primary incident reporting touchpoint can enable impacted entities to share information faster with the federal government and meet reporting requirements.

> "CISA will lead a process…to strengthen processes, procedures, and systems to more fully realize the policy that 'a call to one is a call to all.' When any federal agency receives a request for assistance, [CISA] will know what support the wider federal government can provide, how to contact the right federal agencies that can provide such support, and have access to effective information sharing mechanisms."
>
> - National Cybersecurity Strategy, 2023

While numerous federal agencies and departments have equities during a given cyber incident and need to receive cyber incident data, reporting to each of these entities with their varying requirements is cumbersome for impacted entities. Instead, having a singular point of contact for initial incident reporting can reduce workloads and simplify reporting processes, enabling impacted entities to report more efficiently. Specifically, a tiered process for reporting can allow impacted organizations to meet timelines more effectively while also ensuring that all federal entities receive necessary information.

A lead agency can be the first tier of incident reporting and serve as the initial recipient of time-sensitive information. Having a singular point of contact for initial incident reporting, with clear guidance on the type of information that should be reported, will make it easier for impacted entities to share information with the federal government. The second tier of incident reporting could include follow-up reports for other departments and agencies. Follow-on reporting should account for a more generous timeline for verification and vetting.

SRMAs currently lack the cybersecurity resources to meaningfully function as cyber incident response coordinating bodies.

Ongoing updates to federal cyber policy, notably the National Security Memorandum (NSM) on Critical Infrastructure Security and Resilience, envision an increasingly robust role for SRMAs to coordinate federal response in their sector.[8] However, during the exercise, sector stakeholders and SRMAs alike noted that currently—outside of a few sector-specific relationships including the Department of Defense and the Defense Industrial Base—SRMAs have neither the knowledge nor the resources to play a role in technical incident response coordination in the event of a cyberattack impacting their sector. This is a major gap that should be addressed through policy revisions and resourcing efforts to help SRMAs provide value related to technical incident response.

While some SRMAs may not currently be capable of fulfilling a major role in technical incident response, they would benefit from information sharing related to the cascading impacts of a cyber incident such as a supply-chain disruption. With SRMAs a degree removed from the "cyber" component of a cyber incident, CISA, as the National Coordinator for the Security and Resilience of Critical Infrastructure, should continue to explore processes to provide technical and operational assistance to SRMAs.

Ensuring the confidentiality of information and coordinating with necessary internal parties can slow incident reporting processes.

Some impacted organizations noted that concerns regarding the sensitivity and confidentiality of information limited the nature of their incident-reporting efforts. During an incident, organizations must work through processes to assess what information can be reported and how that reporting can occur. Internal processes that involve consultation with organizational leadership and legal counsel can slow down incident reporting timelines.

Stakeholder-Derived Recommendations:

- The federal government should provide a single incident reporting portal as the first point of contact during a significant cyber incident.
- To ensure ease of reporting and to maintain the quality of information reported, the federal government should offer a condensed and user-friendly reporting form that can be expanded upon later; reporting processes should ensure the confidentiality and integrity of the reported information.
- The federal government should assess how received information can be shared across appropriate agencies and entities; controls should limit availability to agencies and personnel with a need to know.
- If the SRMAs are to take on their designated role as sector incident leads, the federal government must assess the necessary resourcing and appropriate best practices for them to fulfill those roles.
- The federal government should provide information sessions to stakeholders on the types of information that should be reported, triggers for reporting, and security measures taken to ensure information remains anonymized, secure, and confidential.

[8] The White House. National Security Memorandum on Critical Infrastructure Security and Resilience. April 30, 2024.

Finding 5: Federal mechanisms for coordination during significant cyber incidents, as defined in national plans and policies, are not well understood.

Coordination of cyber incident response activities presents significant challenges including varying capabilities and authorities of government agencies as well as the large number of stakeholders involved and the complexity of optimally leveraging their capabilities. The federal government plays a crucial role in cyber incident response, spanning threat response, asset response, and intelligence support activities. During Cyber Storm IX, the federal government designated the scenario a "significant cyber incident," meaning that it was likely to result in harm to the national security interests, foreign relations, economy, public confidence, civil liberties, or public health and safety of the U.S.

National cybersecurity plans and policies define lines of responsibility but leave areas for greater clarity.

To facilitate a coordinated response, Presidential Policy Directive (PPD-41) outlines the principles governing federal response to any cyber incident involving government or private sector entities. For significant cyber incidents, PPD-41 establishes lead federal agencies and an architecture for coordinating the broader federal government response. DHS is the federal lead agency for asset response activities, acting through CISA. The Department of Justice is the federal lead agency for threat response, acting through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force (NCIJTF). The FBI Cyber Division (CyD) is the lead for all aspects of threat response while the NCIJTF, comprising interagency threat response resources, supplements FBI CyD investigative efforts. Additionally, the Office of the Director of National Intelligence (ODNI), through the Cyber Threat Intelligence Integration Center (CTIIC), is the federal lead agency for intelligence support and related activities.

The NCIRP outlines the federal government's responsibilities once a significant cyber incident occurs. It aims to guide the whole-of-nation response to significant cyber incidents and establishes clear lines of authority and responsibility for key agencies and stakeholders. To support the federal government's response efforts to mitigate the impacts of significant cyber incidents, all lead federal agencies must enhance their capabilities to ensure an effective and coordinated response to significant cyber incidents.

All lead federal agencies responsible for cyber incident response and critical infrastructure protection should review their roles and responsibilities outlined in the NCIRP and PPD-41 to ensure an effective and coordinated response to significant cyber incidents. This will help identify any gaps in current plans and policies and enhance the capabilities of federal agencies to mitigate potential impacts of significant cyber incidents on the nation's security, economy, and public health and safety.

Federal agencies could enhance coordination through more proactive information sharing.

During the exercise, participants noted that federal coordination efforts and mechanisms could be improved or clarified. Private sector partners look to CISA, the FBI, and CTIIC for incident support, investigation, and information sharing when faced with a significant cyber threat. While most participants shared information with CISA during the exercise, they were unclear what the federal government would do with this information, and what they could do to assist mitigation and restoration efforts once an incident had been reported. It should be noted that the exercise gave participants the ability to report to the FBI and NCIJTF, but that activity was not as robust as it could have been due to resource constraints.

To enhance their coordination capabilities, federal agencies should exercise and enact formal information-sharing procedures among private sector partners, ISACs, fusion centers, and SRMAs. Participants suggested that establishing a database where trusted representatives from private and public sector organizations can access shared, real-time information about a significant cyber incident would be helpful. Further suggestions

include advanced authentication features and developing new classification markings for public and private sector partner use. Additionally, CISA regions can leverage fusion centers, ISACs, and SRMAs to feed incident information and intelligence from state, local, tribal, and territorial (SLTT) partners up to federal agencies (see Finding 7).

Federal incident scoring processes require additional review.

In the event of a significant cyber incident that impacts federal networks, critical infrastructure providers, or international partners, the federal government needs to assess risk. The National Cyber Incident Scoring System (NCISS) provides a repeatable and consistent mechanism for estimating the risk of a cyber incident.

During Cyber Storm IX, CISA Central convened the NCISS Assessment Cell which leveraged information from CISA divisions and interagency partners to score the cyber incident simulated in the exercise. Both CISA and interagency partners scored this incident as High (Orange) due to the complexity and range of impacts across the U.S. and international partners. While CISA held internal risk assessment discussions with its division leaders and SRMA representatives, resource constraints prevented some key interagency partners from providing their input. This under-resourcing in the exercise indicates a significant concern should real-world conflicts prevent interagency partners from prioritizing an incident.

Adhering to CISA's internal process, federal coordination advanced through the following steps:

1. SRMA representatives provided feedback based on CISA's internal scoring assessment and concurred that this significant cyber incident should be scored as High (Orange).
2. CISA participants including CISA Central, CISA's Cybersecurity Division, and JCDC coordinated their assessments of the incident.
3. JCDC briefed the CRG, held by the National Security Council, with representatives from across federal agencies.

The CRG recommended the establishment of a Cyber Unified Coordination Group (UCG) and provided additional comments based on CISA and interagency NCISS assessments, noting that due to the sheer size of the incident, it should realistically be scored as Severe (Red) instead of High (Orange). Participants indicated that cyber incident scoring methods and actions should be further clarified among CISA and interagency partners. Exercising these cyber incident scoring methods would help clarify roles and responsibilities, create a smoother process for risk assessment discussions, and enable interagency partners to provide further incident information.

Cyber Unified Coordination Group functions should be explored further.

During exercise play, JCDC briefed the CRG on the exercise scenario and their situational assessment based on incident reporting and information sharing among public and private sector partners. Due to time constraints, exercise participants were not able to see the full activation of the Cyber UCG and the additional actions taken by the federal government for asset response, threat response, and intelligence support. Both public and private sector organizations noted that further transparency is needed from the CRG as to what actions will be taken by the federal government once a Cyber UCG is formed.

To clarify the roles, responsibilities, and capabilities of the federal government during a significant cyber incident, exercise participants should consider testing Cyber UCG processes and follow-on actions. This would help enhance the capabilities of federal agencies and provide a better understanding of what actions will be taken by the government to mitigate and restore the effects of a significant cyber incident. Moreover, this would help private sector partners understand the support and assistance they can expect from the federal government.

Stakeholder-Derived Recommendations:

- Lead federal agencies should review roles and responsibilities outlined in the NCIRP and PPD-41.
- Federal agencies should account for how these roles will change following the forthcoming revision of the NCIRP to enhance federal coordination efforts.
- Federal agencies should consider exercising federal coordination procedures with the private sector, ISACs, state fusion centers, and SRMAs; this would enhance coordination efforts and give stakeholders greater trust in the value of collaboration with the federal government during an incident.
- CISA and interagency partners should continue to exercise and review cyber incident scoring plans, policies, and procedures.
- After publication of the updated NCIRP, the federal government should exercise new processes and follow-on actions with a whole-of-government approach that includes private sector partners.

Finding 6: Processes for cyber information sharing between international partners need to mature further.

International coordination on cybersecurity efforts has long been a priority for CISA. Recent documents including the NCS and the NSM on Critical Infrastructure Security and Resilience have underscored the importance of maintaining and improving international collaboration during an incident. Cyber Storm IX provided a unique playing field for CISA and its international partners to assess their information sharing processes and procedures during a global cyber incident. During the exercise, international partners exchanged information, but exercise performance suggests these mechanisms need to be refreshed and more regularly reviewed. Stakeholders noted that sensitivities prevent the sharing of certain types of information (including technical information) between partners and therefore can hinder partners from obtaining a comprehensive understanding of what other nations are encountering during a given incident. This underscores the need to strengthen existing international communication mechanisms.

Twelve countries participated in Cyber Storm IX, creating ample opportunity to test information sharing, communication, and crisis coordination mechanisms. Throughout the exercise, countries dealt with cloud-based impacts to fictional organizations in their respective Food and Agriculture, Financial Services, and Transportation Sectors. Such impacts prompted nations to share high level incident information with international partners, supporting transnational situational awareness.

Existing international information sharing mechanisms work well, but there are challenges posed by the sensitive nature of incident information.

Although Cyber Storm IX exercise play demonstrated that established mechanisms for international communications during an incident are effective, but it also revealed challenges. Participants found they lack appropriate authorities and mechanisms to share sensitive information, including internal technical information and private sector information. The exercise underscored the importance of sharing technical information during a multinational cyber incident while revealing that these sensitivities can hinder information sharing efforts. The NCS describes how international partnerships "can advance common cybersecurity interests by sharing cyber threat information, exchanging model cybersecurity practices, comparing sector-specific expertise, driving secure-by-design principles, and coordinating policy and incident response activities."[9] This highlights the importance of improving cyber threat information sharing policies and practices to more clearly define when and

[9] The White House. National Cybersecurity Strategy. March 1, 2023.

how information—especially technical information—can be securely and efficiently shared with partners. Pursuing such goals would increase global incident response capabilities, benefitting all partners involved.

Streamlining international information sharing practices will help create greater opportunity for collaboration during incidents.

Stakeholders described a level of information sharing during the exercise that provided situational awareness of activity in participating nations but did not lead to comprehensive understanding of the campaign. As noted in NCS Pillar 5, leveraging international coalitions and partnerships among like-minded nations to counter threats to our digital ecosystem through joint preparedness, response, and cost imposition will benefit global cybersecurity.[10] Cyber Storm IX emphasized this by demonstrating how international partnerships use structured information sharing mechanisms during international cyber incidents. The exercise also underscored the importance of streamlining international information sharing during a cyber incident to enable greater collaboration. Without a comprehensive understanding of the issues a given nation is facing, it is difficult for partners to provide useful assistance and/or helpful information. Sharing technical information plays an important role in helping international partners collaborate and respond to a cyber incident. However, when international partners receive information from critical infrastructure sectors, whether by mandatory or voluntary reporting, much of that information is deemed too sensitive to be shared with other countries. Therefore, international partners should look to improve information sharing policies and identify guardrails to better define how information can be shared securely and efficiently.

The U.S. should identify a single primary point of contact for communicating with international partners during a cyber incident.

Cyber Storm IX demonstrated a need to identify a lead agency within the U.S. responsible for communicating with international partners during a cyber incident impacting critical infrastructure. While several offices within CISA collaborate with international partners, there is uncertainty about who should serve as the primary point of contact within the organization for a given incident. CISA should identify a single entity for engagement with international partners during a cyber incident to prevent confusion and streamline information sharing.

Stakeholder-Derived Recommendations:

- International partners should evaluate current information sharing processes and identify specific areas for improvement to promote greater collaboration during an incident; this includes determining a process and guardrails for secure and efficient technical information sharing during a cyber incident.
- CISA should evaluate its international coordination processes and identify a lead for international coordination during a cyber incident.

Finding 7: Stakeholders value the timeliness and familiarity of distributed cyber information sharing networks and believe more could be done to improve their utility.

One of the strategic objectives highlighted in the NCS is to "scale public-private collaboration," which requires strengthening information sharing networks across the country.[11] Both ISACs and fusion centers are integral components of these networks. ISACs collect, analyze, and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resilience, acting as a valuable resource for their sector-specific stakeholders. Fusion centers were created to facilitate better communication and

[10] *Ibid.*
[11] The White House. National Cybersecurity Strategy. March 1, 2023.

cooperation between SLTT law enforcement with federal law enforcement, capabilities that Cyber Storm IX tested when adversaries targeted multiple critical infrastructure sectors. The ability of information sharing bodies like ISACs and fusion centers to disseminate information among federal government, law enforcement, sector-specific, and SLTT entities makes them a key partner in cyber incident response. The Cyber Storm IX scenario highlighted the importance of ISACs and fusion centers while also underscoring the need to improve the timeliness and relevance of shared information during a multi-sector significant cyber incident. As noted in the National Cybersecurity Strategy Implementation Plan, it is important to "investigate opportunities for new and improved information sharing a collaboration platforms, processes, and mechanisms."[12] By enhancing their procedures, practices, and relationships with CISA and each other, ISACs and fusion centers can be better equipped to assist stakeholders to combat threats and attacks.

ISACs are important hubs for information sharing to their communities that need to continue strengthening relationships, broadening memberships, and providing quality information.

ISACs played a unique role in Cyber Storm IX due to their role as information hubs for their specific communities. Because they are sector-specific, ISACs need to expand their membership and strengthen their relationships with members and other ISACs to expand their information gathering and sharing capabilities. By continuing to develop their membership rosters, ISACs can ensure they will obtain more information to analyze and disseminate, thereby improving their capability to support stakeholders across the whole sector. Furthermore, ISACs should strengthen their relationships with CISA and the SRMAs, developing and enhancing information sharing channels and providing higher quality services to their members.

There are sensitivity limitations that restrict how effectively and quickly ISACs can share information that they have received from CISA or have received and are verifying with CISA.

ISACs handle information that is either sensitive to members or sensitive due to classification level, which can hinder timely and effective communications. ISACs need to determine what information they can share and with which members. ISACs should review their current policies and work with CISA to identify processes for sharing information more efficiently.

Enhancing fusion center coordination with stakeholders and ISACs will improve incident response coordination.

Exercise participants believed that fusion centers should be more closely integrated with other cybersecurity information sharing bodies to leverage their relationships more effectively during a cyber incident. Fusion centers have existing relationships with DHS, the FBI, and SLTT governments; developing links to ISACs would ensure increased collaboration and information sharing during cyber and other incidents. During Cyber Storm IX, participants shared information with fusion centers, as they would have during a real incident. Participants noted it is important to further assess the role of fusion centers during a multi-sector significant cyber incident both at the state and national levels. One way to achieve this would be to incorporate additional fusion center participation in future iterations of Cyber Storm.

Strengthening fusion center connections to ISACs and other relevant organizations can benefit overall incident response coordination for all involved entities. CISA should encourage this to further operational collaboration during an incident. A fusion center learning of an incident specific to a certain critical infrastructure sector could reach out to the appropriate ISAC, and vice versa. Leveraging the resources and capabilities of ISACs and fusion centers simultaneously can therefore enhance collaborative cyber incident response coordination.

[12] The White House. National Cybersecurity Strategy Implementation Plan. July 2023.

Fusion centers should be more interconnected to enhance their information sharing and incident response capabilities.

Improving relations between fusion centers will be highly beneficial to stakeholders. Fusion centers vary greatly in their cyber capacity and capability, and such differences can delay or hinder information analysis and dissemination.[13] Because each fusion center has its strengths, improving communication between fusion centers could strengthen overall incident response efforts. This would allow fusion centers specializing in certain areas to provide expertise to counterparts. It would also provide more timely situational awareness for fusion centers located outside of the state where a significant cyber incident is occurring.

The exercise also highlighted the importance of making fusion centers part of the information sharing network. Their unique position as information sharing bodies for SLTT, law enforcement, and federal entities and their existing relationships with these entities make them a valuable partner during an incident. By enhancing fusion center relationships with each other and with other entities, local, state, national, and federal information sharing will be more comprehensive.

Stakeholder-Derived Recommendations:

- ISACs and fusion centers should coordinate with federal entities and reporting members to determine how to best handle information for appropriate, efficient, and secure information sharing.
- ISACs and fusion centers should strengthen their relationships with each other to facilitate more comprehensive information sharing and incident response.
- Fusion centers should improve and expand their relationships to help facilitate more robust and comprehensive information sharing with members and partners.
- CISA should integrate fusion centers into future iterations of Cyber Storm in a greater capacity to account for and exercise their role during a multi-sector significant cyber incident.

Finding 8: In a highly technical and automated field, established relationships are key to effective coordination.

Across the exercise community, stakeholders noted the usefulness of personal connections in facilitating more effective external coordination during incident response. Three examples from the exercise demonstrate the importance of these relationships: the benefit derived when impacted entities have a pre-existing direct relationship with support staff at their cloud service or incident response provider, the preference among state governments for working with known personnel at CISA's regional offices, and the importance of a personal interaction (such as a personalized receipt) following submission of an incident by a critical infrastructure operator to CISA. This last item will become increasingly important in improving compliance as mandatory reporting increases, especially while the incentives or penalties for non-compliance remain undefined.

Direct relationships need to be developed before an incident occurs.

Exercise participants emphasized the value of knowing their incident response partners. This is true of internal incident response, where personal relationships can speed response and reduce intra-organizational friction, and of external coordination, where personal relationships can reduce barriers to initiate communication, leading stakeholders to engage more quickly and be more trusting in their exchange of information, thereby enabling more effective mitigation of the incident. Conversely, not having these relationships in place can reduce exchange of information, delay incident reporting, and impede successful mitigation of an incident. With the

[13] U.S. Department of Homeland Security. National Cyber Incident Response Plan. December 2016.

proliferation of cloud and other managed services, placing key functions outside of the organizational structure and day-to-day operations, external relationships have become more important. To ensure organizations can get the external support they need during an incident, having a communications channel or emergency contact list for these personnel is important.

ISAC events, Sector Coordinating Council meetings, and exercises are all opportunities to make new connections, reinforce old ones, and discuss the appropriate times to engage. These discussions can include the kinds of support that personnel and their organizations offer, how and when to engage that support, and what might be expected in return (such as reporting).

At federal agencies, regional personnel are often the first point of contact.

During the exercise, stakeholders from critical infrastructure and state governments noted that most of their interactions with federal staff occur through regional offices. This is true of interactions with regulators, with SRMAs, and with the federal leads for cyber incident response, CISA and the FBI. This observation supports the NCS intent to bolster regional and field offices for coordination at the local level. [14]

Acknowledgment of incident reporting will improve frequency and quality of reporting.

Increasing requirements for federal cyber incident reporting will allow CISA and other agencies to analyze threats and vulnerabilities across sectors, quickly share relevant information with network defenders across government and the private sector, and warn and protect other potential victims. However, the federal government recognizes that its growing requirements for cyber incident reporting pose a burden to its partners.[15] During the exercise, stakeholders from critical infrastructure and state governments noted that personal acknowledgment of an incident report would help encourage more detailed and expedient reporting.

Stakeholder-Derived Recommendations:

- Organizations should update communications channels and prepare a "break glass" contact list for key internal contacts (including incident response, legal, public affairs, and senior leaders) and external contacts (including CSPs, MSPs, and government partners).
- Federal departments and agencies should continue to resource and empower regional and field offices, in line with evolving doctrine around stakeholder engagement, information sharing, and reporting requirements.
- To drive more frequent, rapid, and detailed incident reporting, CISA and other appropriate federal departments and agencies should continue to educate stakeholders on the incident reporting process, how the information in those reports will be used, and adopt a best practice for issuing a personal acknowledgment of receipt.

[14] The White House. National Cybersecurity Strategy. March 1, 2023, p. 12.
[15] U.S. Department of Homeland Security, Harmonization of Cyber Incident Reporting to the Federal Government. September 19, 2023.

CONSOLIDATED CYBER STORM IX RECOMMENDATIONS

Finding	Recommendations
Finding 1: Collective capabilities and shared responsibilities across stakeholders will ensure that cloud security remains resilient.	Cloud customers should continuously monitor their cloud security configurations and controls, and conduct a thorough assessment of their auditing, logging, identity management, and recovery processes.
	Cloud customers should enact strong security practices (e.g., zero-trust models, key rotation, principle of least privilege) surrounding the creation, use, and monitoring of administrative cloud credentials to maintain the integrity, confidentiality, and availability of cloud-based systems and data.
	Cloud customers should enhance their security baseline using tools such as the CIS benchmark program and should prioritize training staff on cloud security.
	Cloud customers should examine their SLA and work with their CSP to ensure they have the necessary level of service and support in the event of an incident.
	CSPs should provide guidance to customers on secure-by-default blueprints and landing zones, provide security enhancements, and proactively inform customers about risks related to their configurations.
	CSPs should educate customers on the limitations of CSP visibility and access into customers workloads in the event of an incident so they can adjust incident response plans accordingly.
	CISA should continue to provide secure by design guidance and collaborate with CSPs to make security configurations widely available regardless of license tier, as they did with the expanded logging capabilities announced in CISA's Press Release on February 21, 2024.
	Cloud customers should reference the CSA's Cloud Incident Response Framework when incorporating the shared responsibility model into their incident response plans.
	Cloud stakeholders should continue to look to the Federal Risk and Authorization Management Program, a key governance program for the federal government and an influential standard for other sectors, which helps ensure stronger cybersecurity practices, including in cloud-based digital identity, across the cloud service ecosystem.
Finding 2: As incident response planning matures, organizations continue to identify points of failure and challenges linking technical and business response.	Organizations should review incident response plans to ensure roles and responsibilities are clearly defined and to minimize individual points of failure.
	Organizations should establish, document, exercise, and educate staff on incident response communication channels prior to an attack.
	Organizations should develop a primary, alternate, contingency, emergency (PACE) plan that identifies backup methods of communication.
	Organizations' incident response plans should incorporate a list of external collaborators, including capabilities, point of contact, and trigger for contact.
	Organizations should review or exercise processes for engaging MSPs prior to an incident and establish processes where they do not exist.

Finding	Recommendations
Finding 3: Stakeholders could be incentivized to provide more timely reporting of cyberattacks if the federal government facilitated broader, faster information sharing.	The federal government should review parameters and processes for vetting cybersecurity partners and prioritize optimal use of those information sharing relationships.
	The federal government should simplify sensitivity designation and handling instructions for shared information, referencing TLP amber guidance.
	The federal government should review incident report sanitization processes to ensure they are airtight and streamlined to safeguard the reporting entity's anonymity while generating threat information that can be shared with a larger community of stakeholders.
	To ensure the timely sharing of TTPs and IOCs, the federal government should share on a rolling basis, rather than waiting to prepare a full-length report.
	The federal government should continue development and publicization of the Known Exploited Vulnerabilities Catalog as the primary federal repository for up-to-date threat information.
	To overcome institutional barriers to incident reporting, the federal government should drive faster, more detailed, and more frequent incident reporting by developing a standard process to acknowledge reporting, provide protections to the impacted entity, and educate impacted entities on the value they can expect.
Finding 4: The cybersecurity community desires streamlined federal incident reporting structures.	The federal government should provide a single incident reporting portal as the first point of contact during a significant cyber incident.
	To ensure ease of reporting and to maintain the quality of information reported, the federal government should offer a condensed and user-friendly reporting form that can be expanded upon later; reporting processes should ensure the confidentiality and integrity of the reported information.
	The federal government should assess how received information can be shared across appropriate agencies and entities; controls should limit availability to agencies and personnel with a need to know.
	If the SRMAs are to take on their designated role as sector incident leads, the federal government must assess the necessary resourcing and appropriate best practices for them to fulfill those roles.
	The federal government should provide information sessions to stakeholders on the types of information that should be reported, triggers for reporting, and security measures taken to ensure information remains anonymized, secure, and confidential.
Finding 5: Federal mechanisms for coordination during significant cyber incidents, as defined in national plans and policies, are not well understood.	Lead federal agencies should review roles and responsibilities outlined in the NCIRP and PPD-41.
	Federal agencies should account for how these roles will change following the forthcoming revision of the NCIRP to enhance federal coordination efforts.
	Federal agencies should consider exercising federal coordination procedures with the private sector, ISACs, state fusion centers, and SRMAs; this would enhance coordination efforts and give stakeholders greater trust in the value of collaboration with the federal government during an incident.

Finding	Recommendations
	CISA and interagency partners should continue to exercise and review cyber incident scoring plans, policies, and procedures.
	After publication of the updated NCIRP, the federal government should exercise new processes and follow-on actions with a whole-of-government approach that includes private sector partners.
Finding 6: Processes for cyber information sharing between international partners need to mature further.	International partners should evaluate current information sharing processes and identify specific areas for improvement to promote greater collaboration during an incident; this includes determining a process and guardrails for secure and efficient technical information sharing during a cyber incident.
	CISA should evaluate its international coordination processes and identify a lead for international coordination during a cyber incident.
Finding 7: Stakeholders value the timeliness and familiarity of distributed cyber information sharing networks and believe more could be done to improve their utility	ISACs and fusion centers should coordinate with federal entities and reporting members to determine how to best handle information for appropriate, efficient, and secure information sharing.
	ISACs and fusion centers should strengthen their relationships with each other to facilitate more comprehensive information sharing and incident response.
	Fusion centers should improve and expand their relationships to help facilitate more robust and comprehensive information sharing with members and partners.
	CISA should integrate fusion centers into future iterations of Cyber Storm in a greater capacity, to account for and exercise their role during a multi-sector significant cyber incident.
Finding 8: In a highly technical and automated field, established relationships are key to effective coordination.	Organizations should update communications channels and prepare a “break glass” contact list for key internal contacts (including incident response, legal, public affairs, and senior leaders) and external contacts (including CSPs, MSPs, and federal partners).
	Federal departments and agencies should continue to resource and empower regional and field offices, in line with evolving doctrine around stakeholder engagement, information sharing, and reporting requirements.
	To drive more frequent, rapid, and detailed incident reporting, CISA and other appropriate federal departments and agencies should continue to educate stakeholders on the incident reporting process, how the information in those reports will be used, and adopt a best practice for issuing a personal acknowledgment of receipt.

CYBERSECURITY DOCUMENTS REFERENCED IN THE AFTER-ACTION REPORT

Documents Referenced in the After-Action Report
▪ Cloud Security Alliance. Cloud Incident Response Framework. ▪ Cyber Safety Review Board. Review of the Summer 2023 Microsoft Exchange Online Intrusion. March 20, 2024. ▪ Cybersecurity and Infrastructure Security Agency. CISA, OMB, ONCD and Microsoft Efforts Bring New Logging Capabilities to Federal Agencies. February 21, 2024. ▪ National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0. February 26, 2024. ▪ U.S. Congress. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). March 8, 2022. ▪ U.S. Congress. National Defense Authorization Act for Fiscal Year 2021. January 1, 2021. ▪ U.S. Department of Homeland Security. Harmonization of Cyber Incident Reporting to the Federal Government. September 19, 2023. ▪ U.S. Department of Homeland Security. National Cyber Incident Response Plan. December 2016. ▪ U.S. Government Accountability Office. Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods, GAO-23-105468. September 26, 2023. ▪ The White House. National Cybersecurity Strategy. March 1, 2023. ▪ The White House. National Cybersecurity Strategy Implementation Plan. July 2023. ▪ The White House. National Security Memorandum on Critical Infrastructure Security and Resilience. April 30, 2024.

LIST OF ACRONYMS

Acronym	Definition
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act of 2022
CISA	Cybersecurity and Infrastructure Security Agency (within U.S. DHS)
CRG	Cyber Response Group
CSD	Cybersecurity Division (within CISA)
CSP	Cloud service provider
CSRB	Cyber Safety Review Board
CTIIC	Cyber Threat Intelligence Integration Center (within ODNI)
CyD	Cyber Division (within FBI)
DHS	Department of Homeland Security
GAO	U.S. Government Accountability Office
IOC	Indicator of compromise
ISAC	Information sharing and analysis center
ISAO	Information sharing and analysis organization
JCDC	Joint Cyber Defense Collaborative (within CISA)
MSP	Managed service provider
NCIJTF	National Cyber Incident Joint Task Force (within FBI)
NCIRP	National Cyber Incident Response Plan
NCISS	National Cyber Incident Scoring Schema
NCS	National Cyber Strategy
NSM	National Security Memorandum
ODNI	Office of the Director of National Intelligence
PACE	Primary, alternate, contingency, emergency
PPD-41	Presidential Policy Directive 41
SimCell	Simulation cell
SLA	Service-level agreement

Acronym	Definition
SLTT	State, local, tribal, and territorial
SRMA	Sector risk management agency
TLP	Traffic Light Protocol
TTP	Tactics, techniques, and procedures
UCG	Unified coordination group
U.S.	United States

ANNEX A: PARTICIPANT LIST

Critical Infrastructure Participants
Industry Entities
▪ Chemical Sector o Air Liquide US & Airgas o Celanese o Dow o Gallade Chemical ▪ Communications Sector o Charter Communications o Lumen Technologies ▪ Critical Manufacturing Sector o Lennox International o Matthews International o Navistar ▪ Defense Industrial Base Sector o Northrop Grumman Corporation ▪ Energy Sector o Con Edison o Dominion Energy o Shell o Tennessee Valley Authority ▪ Financial Services Sector o American Express o American International Group o Bank of America o BMO Harris Bank o BNY Mellon o Citibank o Fannie Mae o Federal Retirement Thrift Investment Board o Fulton o Independent Community Bankers of America o JPMorgan Chase o Mastercard o Morgan Stanley o Navy Federal Credit Union o PayPal o PNC Bank o SEI Investments Company o State Street o United Services Automobile Association o Wells Fargo o Sumitomo Mitsui Banking Corporation ▪ Food and Agriculture Sector o Albertsons o American Soybean Association o Bunge Corporation o C&S Wholesale Grocers o Cargill o Clean Water Team o CNH Industrial o Coca-Cola

Critical Infrastructure Participants
Industry Entities
○ Compeer ○ Conagra ○ Deere & Company ○ Defense Commissary Agency ○ Festival Foods ○ Food Marketing Institute ○ Heartland Consulting ○ The Hershey Company ○ Hy-Vee ○ International Dairy Foods Association ○ Kroger ○ National Grain and Feed Association ○ National Milk Producers Federation ○ North American Meat Institute ○ Post Holdings ○ Purdue Applied Research Institute ○ Schreiber Foods ○ Shamrock Foods ○ Sheetz ○ Tyson Foods ▪ Healthcare and Public Health Sector ○ Becton, Dickinson and Company ○ Centene Corporation ○ Eli Lilly and Company ○ HCA Healthcare ○ McKesson Corporation ○ Merck ○ Stryker ▪ Information Technology Sector ○ Amazon Web Services ○ Axon Global ○ Blattner Technologies ○ Cisco ○ Crowdstrike ○ Google ○ Grand Canyon Education ○ Guidewire ○ Intel ○ McAfee ○ Microsoft ○ MongoDB ○ Oracle ○ Rackspace ○ SAIC ○ Trellix ○ Upwork ○ Verisign ○ Zscaler ▪ Transportation Systems Sector ○ Fiat ○ Ford ○ General Motors

Critical Infrastructure Participants
Industry Entities
○ Halliburton ○ Honda ○ Hyundai ○ Panasonic ○ Subaru ○ Toyota USA ○ United Parcel Service ○ U.S. Postal Service ▪ Water and Wastewater Sector ○ Arlington County Water Pollution Control Bureau ○ Clark County Water Reclamation District ○ Los Angeles Department of Water and Power ○ Santa Cruz Water Department ○ San Antonio Water Services ○ The York Water Co. ○ Truckee Meadows Water Authority
Coordination Bodies
▪ Arizona Cyber Threat Response Alliance ▪ Automotive Information Sharing and Analysis Center (ISAC) ▪ Aviation ISAC ▪ Cloud Security Alliance ▪ Communications ISAC ▪ Downstream Natural Gas ISAC ▪ Electricity ISAC ▪ Food and Agriculture ISAC ▪ Financial Services ISAC ▪ Health ISAC ▪ Information Technology ISAC ▪ National Council of ISACs ▪ Oil and Natural Gas ISAC ▪ Retail & Hospitality ISAC ▪ The International Association of Certified Information Sharing and Analysis Organizations ▪ WaterISAC

Federal Participants
▪ AbilityOne ▪ Department of Agriculture ▪ Department of Defense ○ DoD Cyber Crime Center ○ National Guard Bureau ○ National Security Agency ○ Office of the Secretary of Defense ○ U.S. Cyber Command ○ U.S. Northern Command ○ U.S. Transportation Command ▪ Department of Homeland Security ○ Customs and Border Protection ○ Cybersecurity and Infrastructure Security Agency ○ Federal Emergency Management Agency ○ Immigration and Customs Enforcement Homeland Security Investigations

Federal Participants
○ Transportation Security Administration ○ U.S. Coast Guard ○ U.S. Secret Service ▪ Department of Commerce ▪ Department of Energy ▪ Department of Health and Human Services ○ Centers for Disease Control and Prevention ○ Indian Health Service ○ Office of the Inspector General ▪ Department of the Interior ○ Bureau of Safety and Environmental Enforcement ○ National Park Service ▪ Department of Justice ○ Computer Crime and Intellectual Property Section ○ DOJ Security Operations Center ○ Justice Management Division ○ Federal Bureau of Investigation ▪ Cyber Watch ▪ National Cyber Investigative Joint Task Force ▪ Department of State ▪ Department of Transportation ○ Federal Aviation Administration ▪ Department of the Treasury ▪ Department of Veterans Affairs ▪ Executive Office of the President ○ National Security Council ○ Office of the National Cyber Director ▪ Federal Communications Commission ▪ General Services Administration ▪ National White Collar Crime Center ▪ Office of the Director of National Intelligence ○ Cyber Threat Intelligence Integration Center ○ Intelligence Community Security Coordination Center ○ National Maritime Intelligence Integration Office ▪ Pension Benefit Guarantee Corporation ▪ Small Business Administration ▪ Securities and Exchange Commission

International Participants
▪ Australia ○ Australian Cyber Security Centre ▪ Canada ○ Canadian Centre for Cybersecurity ○ Public Safety Canada ○ Transport Canada ▪ Finland ○ National Cyber Security Centre/Transport and Communications Agency ▪ Japan ○ Computer Emergency Response Team Coordination Center ○ National Center of Incident Readiness and Strategy for Cybersecurity ▪ Netherlands ○ National Cyber Security Centre

International Participants

▪ New Zealand
  ○ Computer Emergency Response Team
▪ Norway
  ○ National Security Authority/National Cyber Security Centre
▪ Singapore
  ○ Cyber Security Agency
▪ Sweden
  ○ Civil Contingencies Agency/Department of Cybersecurity and Secure Communication
▪ Taiwan
  ○ Ministry of Digital Affairs
▪ United Kingdom
  ○ National Cyber Security Centre

State Participants
State Governments
▪ Commonwealth of Virginia *(observer)* ▪ State of California ▪ State of Hawaii *(seminar)* ▪ State of Illinois *(observer)* ▪ State of Iowa ▪ State of Maine *(seminar)* ▪ State of Minnesota ▪ State of Missouri ▪ State of Nevada ▪ State of New York *(observer)* ▪ State of Rhode Island *(seminar)* ▪ State of Tennessee ▪ State of Texas
Coordination Bodies
▪ Multi-State ISAC (MS-ISAC)

APPENDIX B: EXERCISE DESIGN SUMMARY

Exercise Planning Construct

Cyber Storm IX leveraged the Homeland Security Exercise and Evaluation Program (HSEEP) principles to inform the exercise planning, conduct, and evaluation processes. The Cyber Storm IX planning timeline was divided into five phases that occurred over approximately 18 months, as identified below in Figure B-1.

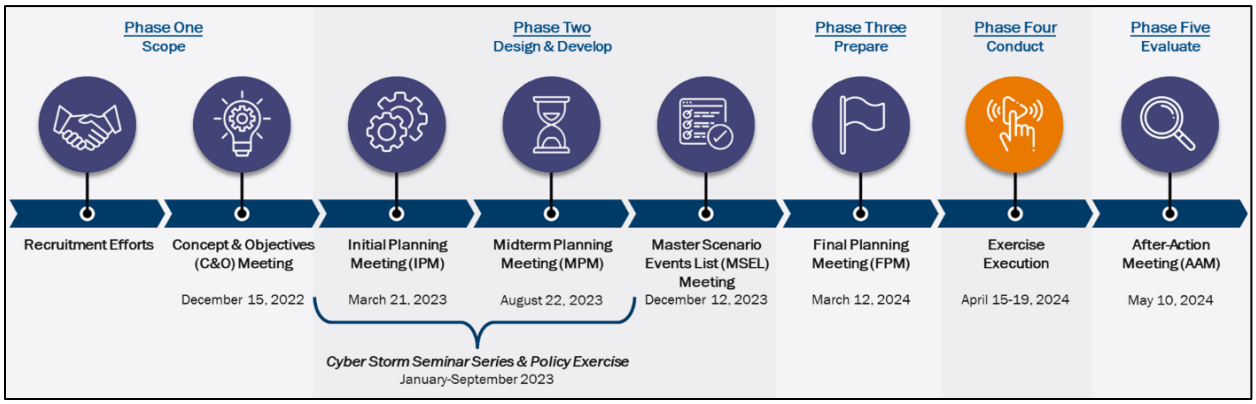

Figure B-1: Cyber Storm IX Exercise Timeline

The Cyber Storm IX Planning Team collaborated with Cybersecurity and Infrastructure Security Agency (CISA) stakeholders to develop Cyber Storm IX over five major planning meetings.

Concept and Objectives Meeting

On December 15, 2022, CISA hosted the Concept and Objectives (C&O) Meeting. Approximately 100 participants and stakeholders from the government and private sector attended the meeting virtually to review and provide input to the Cyber Storm IX concept. The C&O Meeting provided planners with the opportunity to set the stage for a successful Cyber Storm IX by presenting the initial scope and concept of the exercise and facilitating an interactive discussion to gather feedback, gain consensus, and establish next steps. Following this meeting, the Exercise Planning Team initiated recruitment efforts, reengaged previous participants, and continued to define the overall scope.

Initial Planning Meeting

On March 21, 2023, CISA hosted the Initial Planning Meeting (IPM). Approximately 260 participants and stakeholders from the government and private sector attended the meeting to review and provide input to the Cyber Storm IX exercise structure and scenario development. The meeting provided the opportunity to introduce the Cyber Storm IX exercise to new participants and define the desired conditions and outcomes of each organization and Working Group through active participation from organizations' Lead Planners.

Midterm Planning Meeting

On August 22, 2023, CISA hosted the Midterm Planning Meeting (MPM). Approximately 225 participants and stakeholders from the public and private sectors, including international partners, attended the hybrid meeting to review and provide input to the Cyber Storm IX exercise structure and scenario development. The meeting provided the opportunity to review progress made since the IPM, ensure familiarity with future planning milestones, discuss Cyber Storm IX exercise specifics, conduct Cyber Storm IX training, present the core Cyber Storm scenario baseline for discussion, and begin adversary development.

Master Scenario Events List Meeting

On December 12, 2023, CISA hosted the Master Scenario Events List (MSEL) Meeting. Approximately 250 participants and stakeholders from the public and private sectors, including international partners, attended the hybrid meeting to review and provide input to the Cyber Storm IX exercise structure and scenario development. The meeting provided the opportunity to review progress made since the MPM, ensure familiarity with future planning milestones, discuss Cyber Storm IX exercise specifics, conduct Cyber Storm IX training, finalize core scenario elements, and develop the chronological MSEL.

Final Planning Meeting

On March 12, 2024, CISA hosted the Final Planning Meeting (FPM). Approximately 200 participants and stakeholders from the public and private sectors, including international partners, attended the hybrid meeting to review and provide input to the Cyber Storm IX exercise structure and scenario development. The meeting provided the opportunity to review progress made since the MSEL Meeting, provide Cyber Storm IX training, focused on exercise preparation and logistics, ensure familiarity with milestones and requirements for exercise execution, review the exercise scenario events (focusing on timing, cross-sector interaction, and expected player actions), and identify organization-specific scenario gaps.