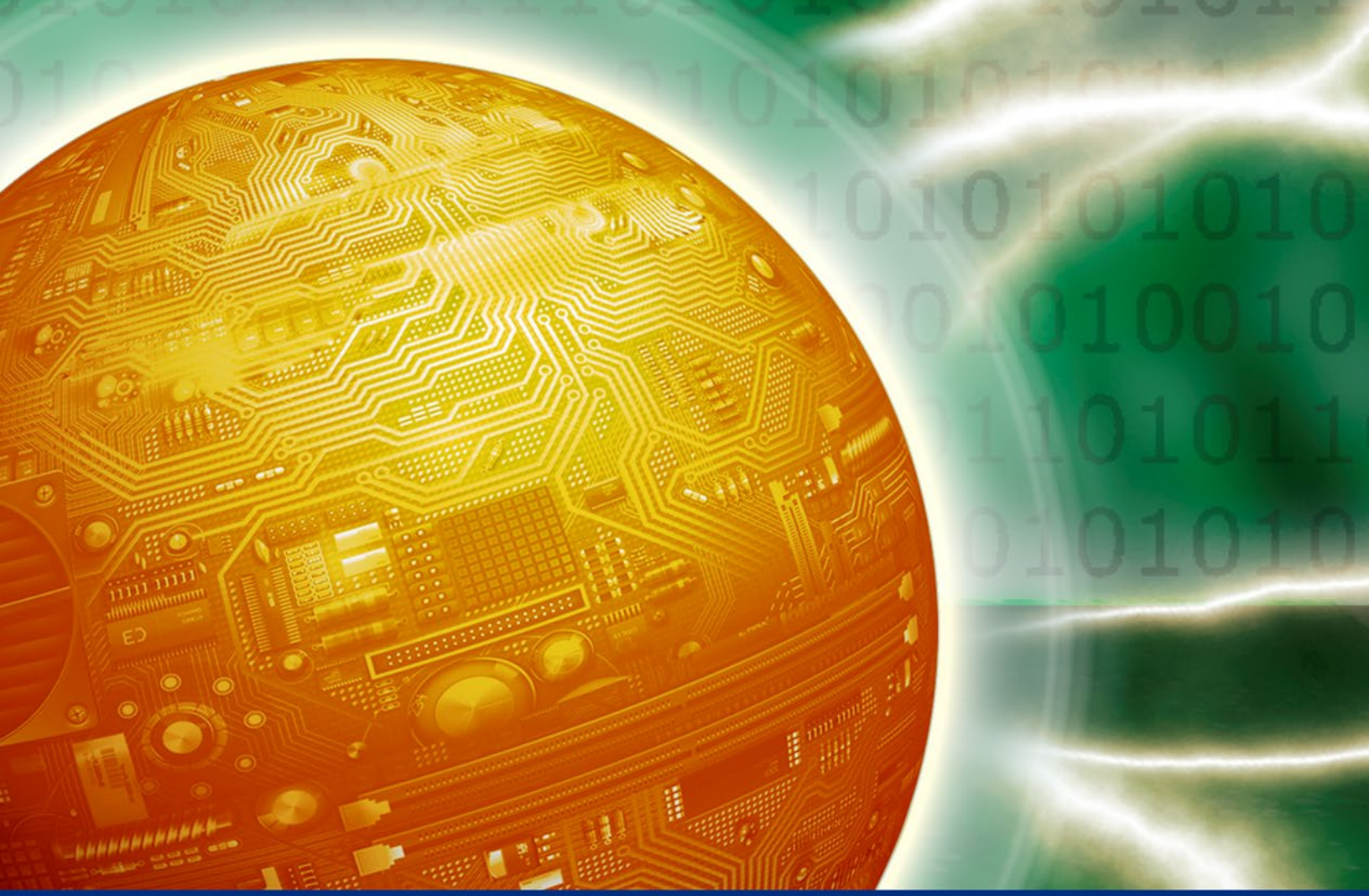

CISA
CYBER+INFRASTRUCTURE

Cyber Storm VI: After Action Report

Cyber Storm VI After Action Report
Table of Contents

EXECUTIVE SUMMARY

Exercise Background

Cyber Storm (CS), the Department of Homeland Security's (DHS) capstone national-level cyber exercise series, provides the framework for the most extensive government-sponsored cybersecurity exercises of their kind. Mandated by Congress, these exercises are part of the Department's ongoing efforts to assess and strengthen cyber preparedness and examine incident response processes. DHS uses the findings to support improvement to collective cyber incident response capabilities. The exercises also strengthen information sharing partnerships and build relationships among federal, state, international, and private sector partners.

The Cybersecurity and Infrastructure Security Agency (CISA) sponsors the Cyber Storm exercise series and these exercises support CISA'a mission to reduce the risk of systemic cybersecurity and communications challenges in the center's role as the Nation's flagship cyber defense, incident response, and operational integration center. CISA successfully executed Cyber Storm VI (CS VI) from its exercise control cell (ExCon) at the United States Secret Service (USSS) Headquarters as well as from distributed player locations from April 9-13, 2018.

The CS VI goal and objectives included:

Exercise Goal:

- Strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector cyber attack targeting critical infrastructure.

Exercise Objectives:

- Exercise the coordination mechanisms and evaluate the effectiveness of the National Cyber Incident Response Plan (NCIRP) in guiding response;
- Assess information sharing to include thresholds, paths, timeliness, usefulness of information shared, and barriers to sharing both internally and externally within the cyber incident response community;
- Continue to examine the role, functions, and capabilities of DHS as the Department coordinates with impacted entities during a cyber event; and
- Provide a forum for exercise participants to exercise, evaluate, and improve the processes, procedures, interactions, and information sharing mechanisms within their organization or community of interest.

The Exercise Planning Team ("Planning Team") divided the 16-month planning process into five phases to support the planning, execution, and evaluation of the CS VI exercise. These included Scope, Design and Develop, Prepare, Conduct, and Evaluate Phases. Within each phase, a series of events, milestones, and planning goals moved the process forward. Five major planning meetings served as key milestones and provided an opportunity for collaboration across the entire planning

community. Throughout the process, planners engaged in cross-community interaction, public–private collaboration, and information sharing to support awareness and achieve goals for each phase.

CS VI exercise execution included more than 2,000 participants, from over 100 individual organizations, representing federal, private sector, state, and international partners. Within the Federal Government, CS VI spanned threat response, asset response, and intelligence support roles and responsibilities—as well as sector-specific responsibilities. Sector participation focused on Communications, Critical Manufacturing, Information Technology (IT), and Aviation and Automotive components of Transportation. Twenty states participated, along with 12 international partners, who focused on Computer Emergency Response Team (CERT)-level coordination. CS VI players ranged from operational shop floor and front-line customer care staff, to security and technical responders, incident response teams, legal and public affairs specialists, and senior leaders.

Key Achievements

CS VI built upon previous exercise achievements, providing an effective venue for learning and advancement. Through the exercise planning and execution process, CS VI:

- Exercised federal, state, private sector, and international response to a significant cyber incident affecting non-traditional IT devices;
- Integrated new stakeholders into a CS national-level capstone, including one new sector, Critical Manufacturing, and one new sector component, Automotive—expanding their exposure to large-scale cyber exercises, supporting relationship-building, and providing a foundation for future exercise and improvement efforts;
- Supported classified planning and execution efforts in coordination with the Intelligence Community Security Coordination Center (IC-SCC) for ICE STORM VII-01-18. During execution, players successfully exercised tear-line processes to share contextual information at the unclassified level with CS VI participants. The joint effort provided realism for players in both exercises as the responses from CS VI were incorporated into ICE STORM play, which informed CS VI player response actions.
- Tested updated international information sharing and communication mechanisms during a cyber incident;
- Raised awareness of the rapidly expanding cyber attack landscape and the nuances of response to incident impacting Internet of Things (IoT) and operational technology (OT) devices;
- Provided a venue for interested states to exercise response to cyber-based impacts affecting the systems and processes that support elections;
- Integrated a simulated and dynamically-updated media and social media platform to replicate the customer and public components of an incident and provided a no-fault learning environment to practice strategies that support this aspect of response;
- Provided an opportunity to examine and identify improvements to internal organizational processes and procedures, including how these may inform or escalate into sector or national-level response; and

- Resulted in positive impact across the participant set. Of respondents to the After Action Questionnaire (AAQ) 98% indicated that participation in CS VI will help them become better prepared to deal successfully with a cyber incident.

Scenario and Adversary

The CS VI core scenario resulted from a simulated vulnerability in an embedded microprocessor used in a wide variety of traditional and non-traditional IT devices. A microprocessor is a computer "brain" on a microchip. Microprocessors are used in everything from the largest mainframes and supercomputers to the smallest embedded systems and handheld devices. Embedded processors are in all traditional and non-traditional IT devices including those played by organizations in the exercise.

The simulated attack against the underlying processor technology allowed for compromises to firmware and software running on these devices, causing widespread scenario impacts across multiple industries, and rapidly rising to a level of national significance. Scenario impacts resulting from the attack included cars being unable to start; robotics on factory floors failing; and IoT devices being leveraged for attacks on corporate or government networks.

The CS VI adversaries incorporated real world threat elements and had the resources, capabilities, and intent to conduct cyber-based attacks on targets in the United States and its allies. Multiple adversary groups used the common vulnerability to develop and deliver exploits targeting exercise participants. This allowed a diverse set of adversary groups to target CS VI players in support of individualized objectives. Attacks ranged from low-level hacktivism style attacks to sophisticated OT infiltration.

Key Findings

Participant feedback and Planning Team observations recorded throughout the exercise planning, execution, and after action process revealed four high-level findings that affect the cybersecurity community at large. High-level findings incorporate perspectives of CS VI participants representing the Federal Government, state and local government, coordination bodies, the private sector, and the international community.

- ***Finding 1:*** ***The cyber attack landscape continues to expand. Attacks that impacted non-traditional IT devices, such as operational technology, highlighted gaps in people, process, and technology; altered the nature of the cyber incident response lifecycle; and emphasized the need for specialized planning and response considerations that support a more comprehensive view of threats.***
- ***Finding 2:*** ***Traditional and social media continue to drive awareness of cyber incidents, while also becoming an increasingly significant component of response. The ability to quickly and effectively engage with customers, stakeholders, and the public; promote***

accurate information over rumor or misinformation; and support efforts to minimize negative brand impact contribute to overall response.

- ***Finding 3:*** ***The National Cyber Incident Response Plan provides a framework for federal coordination but provides for limited linkages to critical infrastructure and the private sector in the early phases of response. This gap creates uncertainty among and within critical infrastructure sectors and may lead to delays or inconsistencies in response.***
- ***Finding 4:*** ***Trusted and established information sharing paths proved to be the most effective during exercise play. Participants who understood their available resources both internally and externally could verify and share data more effectively.***

Conclusion

CS VI provided a realistic environment for participants to assess cyber incident response capabilities. DHS and participating organizations worked closely to scope the exercise and design a realistic scenario that allowed stakeholders to achieve both high-level exercise objectives and their own organizational objectives. The scenario allowed the community to coordinate response to a significant cyber incident that impacted non-traditional IT devices. As part of exercise play, players identified significant findings and areas for improvement at the national, state, sector, and organizational level that the cyber response community should address.

However, the true value of a Cyber Storm exercise is not measured by successful planning and execution, but by the findings, lessons learned, and the actions taken to address identified gaps and areas for improvement. Following CS VI execution, stakeholders will leverage after action reporting in concert with their own internal lessons learned to improve and mature cyber incident response capabilities. DHS will do the same, in partnership with government and industry partners. These improvement actions are critical to increasing the Nation's cyber resiliency and response capabilities.

EXERCISE SUMMARY AND FINDINGS

General Overview

After Action Report Purpose

The Cyber Storm VI (CS VI) After Action Report (AAR) summarizes CS VI and identifies findings and sub-findings that inform Cybersecurity and Information Security Agency (CISA) and stakeholder improvement activities.

CS VI Introduction

Cyber Storm (CS), CISA's capstone national-level cyber exercise series, provides the framework for the most extensive government-sponsored cybersecurity exercises of their kind. Mandated by Congress, these exercises are part of the Agency's ongoing efforts to assess and strengthen cyber preparedness and examine incident response processes. DHS uses the findings to support improvement to collective cyber incident response capabilities. The exercises also strengthen information sharing partnerships and build relationships among federal, state, international, and private sector partners.

The Cybersecurity and Infrastructure Security Agency (CISA) sponsors the Cyber Storm exercise series and these exercises support CISA's mission to reduce the risk of systemic cybersecurity and communications challenges in the center's role as the Nation's flagship cyber defense, incident response, and operational integration center. CISA successfully executed CS VI from its exercise control cell (ExCon) at the United States Secret Service (USSS) Headquarters as well as from distributed player locations from April 9-13, 2018.

Exercise week began on April 9, with exercise participants conducting communications checks and final preparations. Live exercise play kicked off at 9:00 a.m. EDT on April 10, with Assistant Director for Cybersecurity Jeanette Manfra providing opening remarks and sending the first inject. Planners and exercise staff supported core play hours of 9:00 a.m. – 7:00 p.m. EDT each day. Exercise play concluded on April 12 at 5:00 p.m. EDT. During the exercise, DHS and the CS VI Exercise Planning Team[1] ("Planning Team") conducted VIP Tours for senior leadership from across the government and participating sectors. These included an exercise briefing, a live view of exercise play, and an opportunity to meet exercise planners and network. On April 13, planners, players, and stakeholders participated in an exercise Hotwash.

[1] Exercise Planning Team composed of DHS CISA and contractor staff; Team led all aspects of planning, execution, and evaluation

Exercise Objectives

Planners and stakeholders developed the CS VI goal and objectives based on previous exercise experience and findings from Cyber Storms I-V. The goal and objectives are inclusive of community concerns and previous issues, and incorporate current community initiatives. The goal and objectives informed the 16-month planning and execution process. DHS and the Planning Team worked closely with participating organizations throughout the process to achieve the goal and objectives. The CS VI goal and objectives included:

Exercise Goal:

- Strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector cyber attack targeting critical infrastructure.

Exercise Objectives:

- Exercise the coordination mechanisms and evaluate the effectiveness of the National Cyber Incident Response Plan (NCIRP) in guiding response;
- Assess information sharing to include thresholds, paths, timeliness, usefulness of information shared, and barriers to sharing both internally and externally within the cyber incident response community;
- Continue to examine the role, functions, and capabilities of DHS as the Department coordinates with impacted entities during a cyber event; and
- Provide a forum for exercise participants to exercise, evaluate, and improve the processes, procedures, interactions, and information sharing mechanisms within their organization or community of interest.

Exercise Participation

CS VI exercise execution included more than 2,000 participants, representing entities from the public and private sectors within the United States, as well as internationally. These participants represented more than 100 individual organizations across federal, private sector, state, and international partners. CS VI players ranged from operational shop floor and front-line customer care staff, to security and technical responders, incident response teams, legal and public affairs specialists, and even senior leaders.

Within the Federal Government, CS VI spanned threat response, asset response, and intelligence support roles and responsibilities—as well as sector-specific responsibilities. Critical infrastructure sector participation focused on Communications, Critical Manufacturing, Information Technology (IT), and the Aviation and Automotive components of Transportation. Within Critical Manufacturing, organizations included manufacturers within the chemical, consumer products, automotive, machinery, metals, pharmaceutical, and aviation industries. Critical Manufacturing also had representation from the water industry, vendors, and associated government entities. Automotive and aviation participants included automakers, light- and heavy-duty original equipment manufacturers

(OEM), suppliers; a travel company; an airline, and associated government entities. CS VI also included multiple coordination bodies, such as Information Sharing and Analysis Centers (ISAC), Information Sharing and Analysis Organizations (ISAO), and trade associations – focusing on representative bodies for the participating sectors.

Twenty states participated, along with 12 international partners. Of the 20 states, seven participated fully, playing direct scenario impacts and subsequent response to attacks and 13[2] monitored the situation and responded as appropriate. International participation included components of the International Watch and Warning Network (IWWN) and other international partner forums, with a focus on Computer Emergency Response Team (CERT) coordination.

DHS and the Planning Team identified and recruited CS VI participants through leveraging previous CS relationships, reaching out to Government and sector coordination bodies (e.g., Sector Specific Agencies [SSA] and ISACs), and building on past participation. In some cases, participants reached out directly to CISA to express interest in participation. The Planning Team treated all exercise participants as stakeholders, encouraging involvement in defining exercise objectives, developing and applying the scenario conditions, and supporting exercise evaluation. Annex A contains a list of CS VI participants.

Key Achievements

CS VI built upon previous exercise achievements, providing an effective venue for learning and advancement. Through the exercise planning and execution process, CS VI:

- Exercised federal, state, private sector, and international response to a significant cyber incident affecting non-traditional IT devices;
- Integrated new stakeholders into a CS national-level capstone, including one new sector, Critical Manufacturing, and one new sector component, Automotive—expanding their exposure to large-scale cyber exercises, supporting relationship-building, and providing a foundation for future exercise and improvement efforts;
- Supported classified planning and execution efforts in coordination with the Intelligence Community Security Coordination Center (IC-SCC) for ICE STORM VII-01-18. During execution, players successfully exercised tear-line processes to share contextual information at the unclassified level with CS VI participants. The joint effort provided added realism for players in both exercises as the responses from CS VI were incorporated into ICE STORM and ICE STORM play informed CS VI player response actions.
- Tested updated international information sharing and communication mechanisms during a cyber incident;
- Raised awareness of the rapidly expanding cyber attack landscape and the nuances of response to incidents impacting Internet of Things (IoT) and operational technology (OT) devices;

[2] One observing state, New Jersey, participated through the Critical Manufacturing Community

- Provided a venue for interested states to exercise response to cyber-based impacts affecting the systems and processes that support elections;
- Integrated a simulated and dynamically-updated media and social media platform to replicate the customer and public components of an incident and provided a no-fault learning environment to practice strategies that support this aspect of response;
- Provided an opportunity to examine and identify improvements to internal organizational processes and procedures, including how these may inform or escalate into sector or national-level response; and
- Resulted in positive impact across the participant set. Of respondents to the After Action Questionnaire (AAQ) 98% indicated that participation in CS VI will help them become better prepared to deal successfully with a cyber incident.

CS VI Scenario and Adversary

The Planning Team partnered with participants throughout the design process to collaboratively build an exercise scenario that reflected real world threats and would achieve participant objectives. The CS VI core scenario resulted from a simulated vulnerability in an embedded microprocessor used in a wide variety of traditional and non-traditional IT devices. A microprocessor is a computer "brain" on a microchip. Microprocessors are used in everything from the largest mainframes and supercomputers to the smallest embedded systems and handheld devices. Embedded processors are in all traditional and non-traditional IT devices including those played by organizations in the exercise.

The simulated attack against the underlying processor technology allowed for compromises to firmware and software running on these devices, causing widespread scenario impacts across multiple industries, and creating a nationally and internationally significant event. Scenario impacts from the attack included cars unable to start; unusual behavior in factory floor robotics; ransomed devices; and IoT devices leveraged for attacks on corporate or government networks. Within participating organizations, response required collaboration across multiple functional teams within organizations as they tied initial indicators to a cyber source, considered and developed response strategies, and communicated with customers, stakeholders, and the public. Across participating organizations, players shared information with government and law enforcement; coordinated across industries, states, and countries; engaged with vendors; and used information provided in alerts and updates to inform response strategies.

The Planning Team accommodated participant requests for customized elements in line with the core scenario and helped to build logical and technically sound storylines.

For example, two states' Secretary of State offices developed and played scenario elements targeting election systems. State players responded to intrusions on election systems, delays in elections reporting, and social media outrage. This play built redundancies in reporting, integrated response plans with counties and external partners, and refined public communication in preparation for future election cycles.

The CS VI adversaries incorporated real-world threat elements and had the resources, capabilities, and intent to conduct cyber-based attacks upon targets in the United States and its allies. Multiple adversary groups used the common vulnerability to develop and deliver exploits targeting exercise participants. This allowed a diverse set of adversary groups to target CS VI players in support of individualized objectives. Attacks ranged from low-level hacktivism-style attacks to sophisticated OT infiltration.

CS VI Findings

Participant feedback and Planning Team observations recorded throughout the exercise planning, execution, and after action process revealed four high-level findings that affect the cybersecurity community at large. High-level findings and associated discussion incorporate perspectives of CS VI participants representing the Federal Government, state and local Government, coordination bodies, the private sector, and the international community. The Planning Team used the exercise Hotwash, AAQs, CS Community after action teleconferences, and the After Action Meeting (AAM) to build out the findings and supporting evidence. Sub-findings and observations support each high-level finding and provide additional detail.

Finding 1:

The cyber attack landscape continues to expand. Attacks that impacted non-traditional IT devices, such as operational technology, highlighted gaps in people, process, and technology; altered the nature of the cyber incident response lifecycle; and emphasized the need for specialized planning and response considerations that support a more comprehensive view of threats.

1.1 CS VI built awareness of the growing threat landscape, with players observing potential impacts of attacks affecting OT and IoT devices, systems, and technologies, and allowing organizations to consider and practice response. When building and maintaining cybersecurity and information security programs, participants recognized a need to expand the scope to account for both the expansion of potentially vulnerable devices in the ecosystem and the nuances of response to attacks impacting IoT devices.

1.2 Within organizations, players responded to scenario conditions according to established procedures and plans, but in many instances noted the specialized expertise and additional personnel required to respond, and even gaps in plans as players applied them to OT response.

1.3 The scenario highlighted the importance of continuing to raise the level of cyber education and sophistication across organizational staff who may have a part in cyber incident response—especially those outside of operations centers or cyber-focused teams. In a similar scenario, first-line incident responders may reside in customer call centers or on shop floors. Their ability to classify the incident and escalate or share with subject matter experts impacts the speed and ultimately the quality of response.

Finding 1 Observations:

During CS VI, players responded to impacts affecting non-traditional IT devices such as badge readers; heating, ventilation, and air conditioning (HVAC) systems; shop floor machinery and robotics; and even automobiles. The compromise of these devices created significant risks, resulted in substantial operational and economic impacts, and required players to develop creative solutions. For some organizations, especially smaller or less mature participants, CS VI built awareness of this growing threat landscape across the player set and organizational leadership. However, beyond building awareness of potential vulnerabilities, organizations must identify and protect against these risks, as well as prepare for the nuances of response.

Beyond securing traditional enterprise hardware and software, which remains fundamental, organizations increasingly need to adopt a more comprehensive view of potential threats. The scenario and exercise play reinforced the importance of expanding the ecosystem supported by information security and cyber incident response programs to include all types of potentially cyber-vulnerable systems, products, and devices. Standards and guidance continue to evolve and mature. Organizations can leverage existing guidance and resources developed and provided by DHS (including the NCCIC and its expertise in industrial control systems) and the National Institute of Standards and Technology (NIST) to learn more and initiate improvement actions.

Exercise play highlighted gaps that exist when impacted systems and system owners fall outside of established cyber incident response frameworks. In many organizations cyber incident response teams (CIRT) and cybersecurity staff collaborated and managed the incident in partnership with operational staff (e.g., shop floor) or system owners who had expertise on the affected devices and familiarity with associated nuances. In many cases, players established these partnerships and working relationships in an ad hoc fashion, and individuals had limited regular or previous interaction. Cyber incident response planning within organizations would benefit from a continued expansion in focus, incorporating IoT and OT, as well as the teams that maintain and support them.

Exercise play also highlighted opportunities to improve cyber awareness and education. Within organizations, effective response required support and input from multiple functional teams, including staff with limited or no cyber expertise. This was particularly visible during the initial stages of the incident and once players identified and shared patching solutions for organizations to apply to affected systems. For example, many of these attacks created indicators that did not immediately point to a cyber nexus, relying upon the awareness of operators to notify cybersecurity specialists or escalate to cyber incident response teams. For some organizations, it took more time than anticipated to trigger those alerts, as players triaged the issues, considered potential causes, and interacted with affected employees and customers. While CS VI improved awareness of potential cyber vulnerabilities and provided a tangible training opportunity, participants should build upon this success to drive further education across their organizations.

Finding 2:

Traditional and social media continue to drive awareness of cyber incidents, while also becoming an increasingly significant component of response. The ability to quickly and effectively engage with customers, stakeholders, and the public; promote accurate information over rumor or misinformation; and support efforts to minimize negative brand impact contribute to overall response.

2.1 The growth of social media continues to increase the speed and volume of information sharing—valid or invalid. This creates the need to plan for stakeholder engagement in advance, having the capability to quickly release accurate statements, actively consume and validate information, as well as to engage with affected individuals and the public throughout all phases of response. A critical aspect of engagement is the ability to identify and counter misinformation with accurate messaging.

2.2 Media also has the power to drive the narrative, influencing response actions and decisions, particularly as they impact customers, brands, and reputations. In some cases, the issues that the press or the public focus on and drive response to may not align with an appropriate and thorough response. Organizations must consider brand impact as they respond, but also separate brand impact discussions and decisions from technical response activities.

2.3 Social media creates a direct, high-visibility engagement venue. Customers and stakeholders can quickly and publicly report issues and express concerns. Organizations can use social media to their advantage to identify affected customers, directly engage with customers and concerned citizens, and provide guidance. However, many organizations debated the merits versus the potential costs of publicly engaging via social media as they responded to the incident.

Finding 2 Observations:

During CS VI, players engaged on an online platform that contributed to their simulated world view and replicated the realities of a large-scale cyber incident playing out in a public domain. The website

contained mock social media, traditional media, and press release pages. This dynamic environment simulated customer complaints, public commentary, media inquiries and subsequent coverage, as well as adversary commentary and communications. These inputs allowed organizations to practice developing and delivering messaging while under the stress of managing response efforts. Players also identified affected customers, countered inaccuracies, and used the online dialogue to inform aspects of their response. Law enforcement and intelligence players leveraged the adversaries' online footprint to investigate the attacks, and ultimately seized the infrastructure and arrested multiple suspected attackers.

The high-impact, public-facing scenario highlighted the importance of managing the brand and considering reputation and public perception throughout response. This required communicators to be heavily involved in response and challenged existing review and approval processes and timelines for public releases (i.e., days to hours). Participating organizations identified a need to streamline processes for public releases in high profile events and develop pre-approved holding statements or templates to accompany cyber incident response plans.

Players and planners observed the importance of getting messages out quickly to get ahead of or counter rumor and misinformation—even if that messaging is simply acknowledging a potential incident, providing simple facts, and alerting to ongoing investigatory efforts. Inaccurate information, intentionally planted or inadvertently cited, can lead to false conclusions. Despite lacking a factual basis, misinformation and bad information can take on a life of its own, trend on social media, and get picked up by traditional media. The effort required to identify and "drown out" bad information once it is out there and has gained steam is significantly more difficult that taking a proactive and fact-based approach from the start.

Multiple stakeholders observed that the public coverage impacted response efforts more than they anticipated. For example, planners observed cases where discussions regarding brand impact or negative perception detracted from or delayed technical response efforts. In other cases, leaders altered guidance on response strategies based on customer complaints, public commentary, and media coverage. Though there is value in being agile and responsive to the customer base and the public, organizations should ensure that decisions on technical response strategies are based on sound, accurate technical information and recommendations. While there must be a connection between the two efforts, stakeholders recommended maintaining two separate work streams staffed by appropriate subject matter experts.

Government participants, especially those from non-DHS SSAs, observed an opportunity to improve the whole-of-government messaging during a cyber incident and limited existing national-level guidance. Post-exercise, these planners discussed the potential value of coordinating messaging

efforts across involved government departments and agencies. In a similar scenario, the government can provide an objective voice and assist in efforts to validate and manage the facts.

Finding 3:

The National Cyber Incident Response Plan provides a framework for Federal coordination but provides for limited linkages to critical infrastructure and the private sector in the early phases of response. This gap creates uncertainty among and within critical infrastructure sectors and may lead to delays or inconsistencies in response.

3.1 Federal players representing the Intelligence Community and Federal Cyber Centers demonstrated improved ability to quickly declassify and release contextual information to uncleared audiences. In cooperation with ICE STORM VII-01-18, participants successfully coordinated and shared information with CS VI players in accordance with the NCIRP, Presidential Policy Directive (PPD)-20 and PPD-41.

3.2 Players leveraged internal incident response plans and exercised external reporting requirements and coordination mechanisms. However, outside of federal entities with NCIRP-designated roles and responsibilities, the diverse participant community did not leverage a cohesive or common framework to guide incident response activities at a national-level, particularly when it came to decision-making, escalation processes, or development and distribution of large-scale remediation strategies across the diverse player set.

3.3 During significant cyber incidents, the Cyber Unified Coordination Group (UCG) serves as the primary national operational coordination mechanism between and among federal agencies, and is also the mechanism to integrate private sector; critical infrastructure; and state, local, tribal, and territorial (SLTT) communities. However, this operational framework requires pre-incident planning to identify the proper escalation and communications paths, particularly for SSAs. Participants used CS VI to initiate some of these activities, but more effort is needed to ensure that stakeholders have appropriate expectations and can easily leverage these mechanisms in crisis.

3.4 Unlike previous iterations, the Cyber UCG as defined in the current NCIRP (i.e., December 2016 version) does not provide a direct mechanism to engage the private sector. This change resulted in many private sector partners questioning if the government would contact them during a cyber incident and how affected sectors may be engaged. Processes need to be clearly defined as to how the government plans to engage the private sector.

Finding 3 Observations:

Historically, the Intelligence Community relied on a system of declassifying and releasing only the most basic information—including Indicators of Compromise (IOC) and Indicators of Attack (IOA) information—often without sufficient context. Conversely, during ICE STORM VII-01-18 and CS VI, participants successfully coordinated to declassify aspects of the intelligence valuable to responders and shared this information with CS VI players in accordance with the NCIRP, PPD-20,

and PPD-41. This release of tear-lined contextual information to the Federal Cyber Centers allowed for the timely dissemination of government and private sector threat information through subsequent products and alerts (e.g., NCCIC Alert). These products and alerts informed response operations and public messaging activities.

In accordance with PPD-41, DHS led the development of a refreshed NCIRP, releasing it in December 2016. The refreshed NCIRP retains many of the principles from the 2010 version and clarifies concurrent lines of effort. Players, particularly those from the Federal Government, exercised coordination and escalation aspects of the NCIRP during CS VI. However, due in part to time constraints and in part due to an increased focus on federal escalation and coordination during the initial stages of an incident, the SSAs and private sector organizations had limited ability to exercise and improve operational familiarity with the framework. Players outside of the Federal Government did not truly leverage a cohesive or common framework to engage within incident response activities at a national-level; they relied on internal plans and external reporting requirements. Planners observed opportunities to review internal plans and requirements and include escalation processes and external engagement guidance.

Per the NCIRP, the "relevant sector-specific agency will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure." During the exercise, players from DHS NCCIC, Federal Bureau of Investigation (FBI) National Cyber Investigative Joint Task Force (NCIJTF), and Office of the Director of National Intelligence (ODNI) Cyber Threat Intelligence Integration Center (CTIIC) conducted a preparatory call among action officers. After determining the incident to be a significant cyber incident, they proposed members of a Cyber UCG and identified SSAs to integrate. However, due to time constraints and an ongoing real-world incident, a full Cyber UCG standup did not occur during exercise play. As a result, SSAs expressed uncertainty regarding the process, including expectations for them and from the Cyber UCG. Moving forward, participating SSAs identified a need to conduct pre-planning to facilitate integration of affected private sector critical infrastructure. Pre-planning efforts should identify the proper points of contact, clarify the need for sector coordination efforts to precede a Cyber UCG, and establish a shared understanding of expectations.

Beyond the SSAs, multiple private sector stakeholders commented that they had limited insight into the government's priorities and assessment of the threat level during exercise play. As the owners and operators of much of the Nation's critical infrastructure, many private sector stakeholders felt they might have been able to assist the government if they had awareness of government needs. They expressed interest in exploring options for further dialogue or coordination, especially during the early stages of an incident. In the previous iteration of the Cyber UCG, public and private sector stakeholders met regularly at a "staff-level" to discuss issues and share a common operating picture.

Something like this may have value in the future to facilitate dialogue and familiarity. Participants also shared that ISACs and private sector entities with liaison officer (LNO) positions at the NCCIC conducted valuable public-private and inter-sector coordination, even facilitating further two-way information sharing with ISACs without LNO seats. This may be another mechanism to facilitate public-private engagement.

Finding 4:

Trusted and established information sharing paths proved to be the most effective during exercise play. Participants who understood their available resources both internally and externally could verify and share data more effectively.

4.1 The diverse nature of the CS VI participant set, including the participation of multiple information sharing and analysis organizations, highlighted the value of information sharing models organized around established, trusted communities of interest.

4.2 CS VI highlighted the criticality of intra-sector relationships to drive coordination and information sharing. Within the CS VI player set, sector ISACs provided an effective and trusted venue to coordinate and share information for affected and unaffected member organizations. ISACs could then coordinate amongst themselves and with national and federal organizations, such as the NCCIC or the FBI.

4.3 Through both the planning and execution phases, many CS VI participants identified new and strengthened existing information sharing relationships. New relationships span from an increased awareness of existing resources (e.g., subscribing to NCCIC Alerts or FBI Private Industry Notifications [PIN]) to participants exploring more formalized standard operating procedures (SOP) as an outcome of exercise play. For existing relationships, many participants strengthened their collective trust and familiarity and increased their understanding of information needs and requirements.

Finding 4 Observations:

During the exercise, organizations leveraged information sharing and analysis organizations based on their community of interest to share information on the unfolding cyber incident. For example, pharmaceutical manufacturers coordinated with the National Health Information Sharing and Analysis Center (NH-ISAC), chemical manufacturers leveraged the American Chemistry Council (ACC), states engaged via the Multi-State Information Sharing and Analysis Center (MS-ISAC), affected nations communicated across the IWWN, and OEMs and suppliers utilized the Auto-ISAC. Many participants commented on the utility of intra-ISAC member interactions on conference calls and associated products received via notifications. From there, ISAC leaders, National Council of ISACs (NCI) analysts, and liaison officers sitting within the NCCIC facilitated further coordination and information sharing across sectors. This contributed to greater awareness of the "big picture" for the ISACs and their member organizations.

Beyond these many positive interactions, several participants did comment that while information sharing between ISACs has improved significantly, there is still room for improvement, with some players anticipating more information during the exercise. In some instances, ISAC players indicated that expanded information sharing could have enhanced response. This may have been due in part to an exercise artificiality, with CS VI not simulating a full NCI spin-up.

Beyond highlighting the value of this existing information sharing model for member organizations, the CS VI scenario revealed gaps that exist when organizations do not align to an ISAC or ISAO. Many of these organizations leveraged peers, vendors, working groups, law enforcement, and federal agencies when a relationship existed. While these informal relationships provided value, organizations had fewer opportunities to coordinate, develop shared situational awareness, or integrate within response at a community and national-level. Organizations should continue to look for opportunities to engage externally, building or strengthening relationships to benefit downstream incident response.

In recent years, Automotive and Critical Manufacturing participants both matured their cybersecurity stance, improving awareness of threats, building industry relationships, and establishing formal and informal information sharing channels. The planning and execution of CS VI provided a venue to build and strengthen relationships and an opportunity to evaluate operational response. During execution, organizations shared information where established relationships or venues existed, but at times noted that their players focused primarily on internal response, missing commonalities in attacks and impacts across similar organizations, and losing opportunities to explore potential efficiencies. Participants identified improvement actions within their organizations and across the industries, including interest in expanding coordination efforts and participating in similar events.

As an exercise that focuses on the policy and procedure aspects of response, information sharing is always an important factor during execution and in evaluation. Exercise play helped to illuminate gaps that delayed or challenged communications. For example, participants observed and reinforced the importance of effective practices, such as updating point of contact lists at regular intervals and identifying and training backups for key roles. Within states, multiple participants observed challenges in sharing information across agencies due to uncertainty about information requirements, authorities, and processes. Some players, especially on the international front, identified areas where access issues challenged information sharing and need to be addressed as an outcome of CS VI play. Many of these participants are already using these takeaways to streamline information sharing in the future.

Exercise Design Summary

Exercise Planning Construct

The Planning Team divided the 16-month planning process into five distinct stages to support the planning, execution, and evaluation of the CS VI exercise (figure 1). Within each stage, a series of events, milestones, and general planning goals advanced the exercise forward. Throughout the process, planners shared information and actively collaborated within and across communities and between the public and private sector stakeholders.

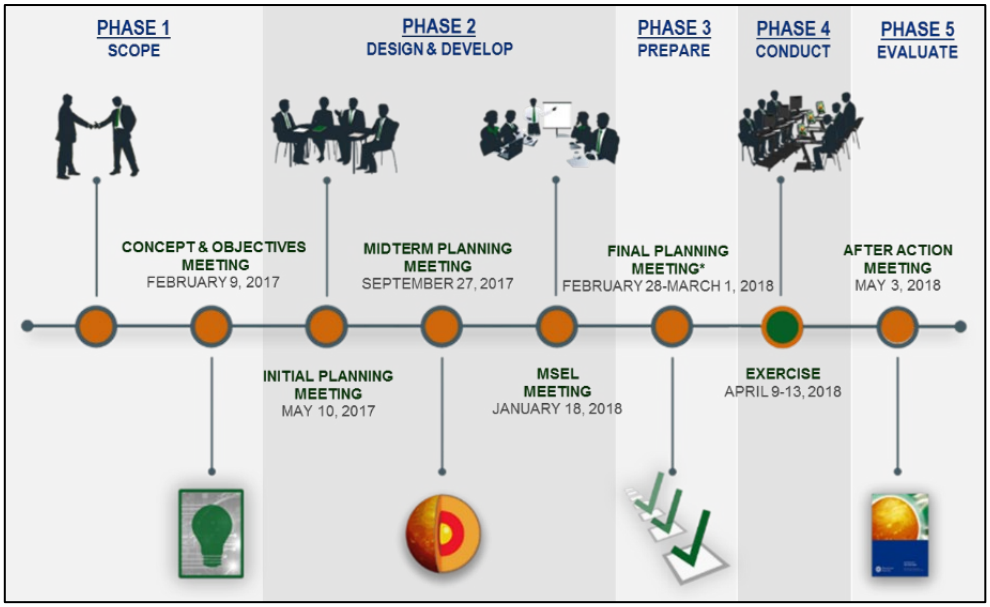

Figure 1: CS VI Occurred Over Five Phases

Scope Phase

To kick off planning efforts DHS and the Planning Team collaborated on the proposed exercise concept, to include identifying the scope, goal and objectives, timeline, and potential sectors. Efforts focused on establishing the conceptual framework to set the stage for initial discussions with potential stakeholders. On February 9, 2017, DHS hosted the Concept and Objectives (C&O) Meeting to discuss the proposed CS VI scope and solicit input. At the meeting, nearly 45 stakeholders and participants discussed the goal and objectives, planning and execution timeline, recruitment targets, scenario options, and exercise structure and design principles. Following this meeting, the Planning Team initiated recruitment efforts, reengaged previous participants, and continued to define the overall scope based on feedback from the C&O Meeting.

Selecting critical infrastructure sectors comprised an important milestone in this phase. CS exercises include at least two sectors in addition to traditional IT and Communications Sector participants. This participation model integrates new players, builds new and strengthens existing relationships, and improves cyber response plans and capabilities. CS VI sector criteria included perceived readiness, interest and ability to commit, DHS relationships, IT and Communications dependencies, applicability to exercise concept, and a threat analysis of recent attacks and future threats. The first sector, Critical Manufacturing, expressed interest in participating and had been impacted by recent proliferation of attacks. Beyond these factors, DHS serves as the SSA. Within the Transportation Sector, the Planning Team focused on two components, automotive and aviation. A combination of DHS serving as the sector's Co-SSA, advancements in information sharing organizations, and growing vulnerabilities made them ideal candidates.

To support efficient design, the Planning Team utilized the "CS Community" approach to exercise planning. As participants on-boarded, they joined a focused CS Community, each with a dedicated Planning Team Lead. The CS Communities created forums to discuss common issues and identify scenario impacts to challenge their players. The CS VI Communities included Critical Manufacturing, Transportation, Federal, International, IT/Communications (IT/Comms), Law Enforcement/Intelligence/Department of Defense (LE/I/DoD), and States.

Design and Develop Phase

The Design and Develop Phase comprised most of the planning process and included three of the five major planning meetings. During this phase, the Planning Team and organizational planners finalized the exercise's goal and objectives, defined boundaries and desired conditions, identified players, developed the scenario and adversary, and applied these to organizational conditions to create scenario injects. In addition, the organizational planners participated in monthly CS Community calls, received virtual training on CS VI, and led all organization-specific aspects of exercise planning.

DHS hosted the Initial Planning Meeting (IPM) on May 10, 2017, for nearly 100 stakeholders. The full-day meeting consisted of a series of both plenary and breakout sessions designed to provide information on exercise construct and solicit input on design specifics. For many of the stakeholders, the IPM was the first chance to gain an understanding of the exercise scope and construct. The plenary sessions informed stakeholders of the timeline, associated milestones, planner responsibilities, and the scenario planning process. CS Communities used breakout sessions to scope the participant set, plans and policies, potential attack vectors, and scenario boundaries.

Following the IPM, CS VI stakeholders identified organization-specific objectives, scenarios of interest, and additional partners and players to recruit for the exercise. A Scenario Team, comprised of key technical and exercise professionals, began to design the exercise core scenario to serve as the

technical basis for exercise play. The International Community also stood up immediately following the IPM. Communities held monthly teleconferences throughout the planning process to provide updates and advance community and scenario development. In many cases, CS Community Leads also held one-on-one calls with organizations to conduct more focused working sessions on each organization's exercise play.

On September 27, 2017, DHS hosted the Midterm Planning Meeting (MPM). Nearly 100 stakeholders attended the full-day meeting. MPM sessions provided information on planning progress and milestones, described the core scenario baseline, initiated community scenario planning, and solicited input on exercise design specifics. The core scenario baseline would become the unifying backstory of the local impacts on each CS Community. At the conclusion of the MPM, the Planning Team provided information on exercise resources, logistics, the after action process, and initial public affairs guidance on CS VI external messaging.

After the MPM stakeholder organizations built out their internal scenarios using the core scenario as a baseline. Community Leads assisted organizations in tying the core scenario baseline to common organizational desired conditions via pre-identified scenario linkages. Developing these scenario linkages ensured that the scenarios made logical technical sense and triggered the national-level discussions. They also ensured CS Community members experienced similar conditions to similar systems. Coming out of this process, each organization had a scenario framework established that could be shared with other stakeholders in their community and be further refined into the observable injects presented to players during the exercise.

DHS hosted the Master Scenario Events List (MSEL) Meeting on January 18, 2018. At the meeting, the Planning Team led nearly 130 attendees through a full-day of both plenary discussions and CS Community-focused breakout sessions. The plenary discussions covered exercise structure, scenario development, timing, and inject development. The community-focused breakout sessions focused on how the timing of scenario events manifest across the three days of the exercise. During subsequent plenary sessions, all exercise stakeholders discussed the timing of scenarios and cross-community exercise play. Additional MSEL Meeting briefings provided planners with information on adversary connections, exercise resources and evaluation, public affairs guidance on CS VI external messaging, and the VIP Program.

Building on the MSEL Meeting, CS Communities finalized organization-specific scenario narratives. Using the narratives, planners identified their player observables and developed time-sequenced exercise injects. The sum of the exercise injects for each organization became their MSEL. To be fully prepared for exercise play, planners also identified expected player actions, organizational media play, and simulation requirements for ExCon. CS Community Leads continued to host monthly

planning calls as well as individual calls with organizations to update their MSEL in preparation for the Final Planning Meeting (FPM).

Prepare Phase

As the fifth and final major planning meeting, DHS hosted the Final Planning Meeting (FPM) on February 28 and March 1, 2018, for nearly 140 stakeholders. The first day consisted of a full-day of plenary discussions focused on exercise scenario events, inject timing, cross-sector interaction, and expected player action. These discussions ensured that the scenario ground truth remained in sync across all communities. Additional FPM briefings focused on real world and exercise-related public affairs, the VIP Program, logistics, and mechanics to prepare planners for exercise execution.

On the second, optional day of the FPM, the Planning Team provided training on the exercise website, including information on the registration process and the platform's components and functions. The second day also provided opportunities for voluntary working sessions with CS Community Leads. Communities reviewed injects and projected timelines and discussed scenario impacts and expected player actions. These sessions allowed planners to delve into injects and timing as they related to the broader exercise overview from the day prior.

The Planning Team prepared planners by sharing information on ExCon logistics, assisting with artifact development and contingency inject review, identifying white cell support roles, and finalizing the Player Phone Book. Community Leads coordinated working sessions with members of the Scenario Team and organizational planners to edit and ultimately finalize exercise injects. The Planning Team also provided eight virtual "Planner and Controller/Evaluator (C/E) Training" sessions and 17 sessions of virtual "Player Training." Planner and C/E sessions provided guidelines for observing exercise play and described roles and responsibilities before, during, and after CS VI. Player sessions introduced and familiarized players with the exercise and described their role and available resources during the exercise.

Conduct Phase

CS VI exercise execution included thousands of participants, representing entities from the public and private sectors within the United States, as well as internationally. Exercise participants included players, C/Es, and ExCon representatives. DHS hosted approximately 100 representatives at CS VI ExCon, in Washington, D.C., from April 9 to 13, 2018. ExCon functions included exercise management; flow control; inject review, development, and release; and simulation support. ExCon representatives included participants from the public sector, private industry, critical infrastructure sectors, and states. These representatives helped to manage play at their own organizations through interaction with other ExCon members and contact with their offsite C/Es.

On the first day, ExCon and participants out in the field conducted systems checks, reviewed read-ahead material, and prepared for live exercise play. Live exercise play ran from 9:00 a.m. on Tuesday, April 10, until 4:00 p.m. EDT on Thursday, April 12. During this time, ExCon distributed more than 1,400 pre-scripted injects via email and phone calls. Players received additional ad hoc injects based on player response and exercise play. The Exercise Website allowed registered users to access exercise documentation, the Player Phone Book, and simulated social and traditional media. Players accessed adversary sites and blogs through a separate platform. The Planning Team updated all simulated sites in real time during the exercise based on dynamic play.

During exercise play, ExCon also facilitated twice-daily "All-ExCon and C/E Teleconferences" to summarize scenario play, preview upcoming activity, discuss initial observations, and answer questions. On Friday, April 13, 2018, ExCon representatives, distributed C/Es, and local stakeholders conducted the Hotwash. During the Hotwash, the Planning Team reviewed overall exercise play, and all participants discussed exercise outcomes and initial findings. The Planning Team provided additional information on next steps, the after action process, and reminded all participants to submit an AAQ.

Evaluate Phase

The Planning Team implemented various mechanisms to capture player action, observations, and evaluation input. Participating organizations provided a C/E to monitor and control exercise play from that organization's home location. During CS VI, C/Es reported on scenario development, monitored player interaction, and communicated issues. C/Es also participated in twice-daily teleconferences to remain in sync and informed of upcoming scenario activity. The Planning Team encouraged C/Es to use an "Evaluation Guide," available on the Exercise Website, to guide internal tracking and evaluation efforts. After live exercise play concluded, DHS encouraged all participants to complete and submit an AAQ. There was a Player-specific AAQ and a Planner and C/E-specific AAQ with tailored questions. The AAQs captured feedback on key takeaways, external interaction, the effectiveness of exercise alerts, and strengths and areas for improvement from exercise play. The AAQs also captured input on the CS VI planning and execution process.

After Action Questionnaire Highlights

- ✓ 99% of respondents found participation in CS VI to be a valuable experience
- ✓ 98% of respondents indicated that participation in CS VI will help them become better prepared to deal successfully with a cyber incident

DHS hosted several after action events to discuss and vet potential findings and to solicit feedback from the participant community. First, each CS Community hosted a teleconference to discuss community-specific findings, observations, and feedback. On May 3, 2018, DHS hosted the AAM for

all exercise participants both in-person at DHS and via teleconference. During the meeting, attendees reviewed and provided input on high-level findings, sub-findings, and recommendations for improvement. Following the AAM, the Planning Team provided participants with several opportunities to review and provide edits to the after action documentation.

Conclusion

CS VI provided a realistic environment for participants to assess cyber incident response capabilities. DHS and participating organizations worked closely to scope the exercise and to design a realistic scenario that allowed stakeholders to achieve both high-level exercise objectives and their own organizational objectives. The scenario allowed the community to coordinate response to a significant cyber incident that impacted non-traditional IT devices. As part of exercise play, players identified significant findings and areas for improvement at the national, state, sector, and organizational level that the cyber response community should address.

However, the true value of a Cyber Storm exercise is not measured by successful planning and execution, but by the findings, lessons learned, and the actions taken to address identified gaps and areas for improvement. Following CS VI execution, stakeholders will leverage after action reporting in concert with their own internal lessons learned to improve and mature cyber incident response capabilities. DHS will do the same, in partnership with government and industry partners. These improvement actions are critical to increasing the Nation's cyber resiliency and response capabilities.

ANNEX A. PARTICIPANT LIST

Cyber Storm VI Participants
Federal Government Entities

• Central Intelligence Agency (CIA)
• Department of Commerce (DOC)
  ○ Bureau of Economic Analysis (BEA)
  ○ National Institute of Standards and Technology (NIST)
  ○ National Oceanic and Atmospheric Administration (NOAA)
  ○ National Telecommunications and Information Administration (NTIA)
• Department of Defense (DoD)
  ○ Defense Security Service (DSS)
  ○ Department of Defense Cyber Crime Center (DC3)
  ○ Missile Defense Agency (MDA)
  ○ National Guard Bureau (NGB)
  ○ National Security Agency (NSA)
  ○ Office of the Secretary of Defense for Policy (OSD-P)
  ○ United States Cyber Command (USCYBERCOM)
  ○ United States Northern Command (USNORTHCOM)
• Department of Energy (DOE)
  ○ Joint Cybersecurity Coordination Center (iJC3)
  ○ National Nuclear Security Administration (NNSA)
  ○ Office of the Chief Information Officer (OCIO)
• Department of Justice (DOJ)
  ○ Federal Bureau of Investigation (FBI)
  ▪ Bureau Intelligence Council
  ▪ Cyber Division
  ▪ Enterprise Security Operation Center (ESOC)
  ▪ National Cyber Investigative Joint Task Force (NCIJTF)
  ▪ Cyber Watch (CyWatch)
• Department of Health and Human Services (HHS)
  ○ Administration on Children and Families (ACF)
  ○ Centers for Disease Control (CDC)
  ○ Centers for Medicare and Medicaid (CMS)
  ○ Food and Drug Administration (FDA)
  ○ National Institutes of Health (NIH)
  ○ Office of Security and Strategic Information (OSSI)
  ○ Office of the Chief Information Officer (OCIO)
• Department of Homeland Security (DHS)
  ○ National Protection and Programs Directorate (NPPD) (now the Cybersecurity and Infrastructure Security Agency (CISA))
  ▪ National Risk Management Center
  ▪ Office of General Counsel Cybersecurity (OGC-Cyber)
  ▪ Office of Cybersecurity and Communications (CS&C)
  • Federal Network Resilience (FNR)
  • Office of the Assistant Secretary (OAS)
  • National Cybersecurity and Communications Integration Center (NCCIC)
  • Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR)
  ○ Office of External Affairs
  ○ Office of Infrastructure Protection (IP)
  ▪ National Infrastructure Coordinating Center (NICC)
  ▪ Sector Outreach and Programs Division (SOPD)
  ○ Transportation Security Administration (TSA)

Cyber Storm VI Participants
○ United States Coast Guard (USCG) ○ United States Immigration and Customs Enforcement (ICE) ▪ Homeland Security Investigations Cyber Crimes Center (HSI/C3) ○ United States Secret Service (USSS) • Department of Transportation (DOT) ○ Federal Aviation Administration (FAA) ○ National Highway Traffic Safety Administration (NHTSA) ○ Volpe Center • Department of Veterans Affairs (VA) ○ Office of Information Security (OIS) • Office of the Director of National Intelligence (ODNI) ○ Cyber Threat Intelligence Integration Center (CTIIC) ○ Intelligence Community Security Coordination Center (IC-SCC)
State Government Entities
Fully Participating States: • Colorado ○ Arapahoe County ○ Colorado Secretary of State ○ Denver County ○ Governor's Office of Information Technology ○ Jefferson County • Delaware ○ Delaware Department of Emergency Management ○ Delaware Department of Transportation ○ Delaware State Police ○ Delaware Information and Analysis Center (DIAC) ○ Department of Technology and Information ○ JP Morgan Chase ○ Morris James • Iowa ○ Iowa Workforce Development ○ Office of the Chief Information Officer • Montana ○ Department of Public Health and Human Services ○ Department of Revenue ○ State Information Technology Services Division • Texas ○ Department of Public Safety ○ Texas Commission on Environmental Quality ○ Texas Education Agency ○ Texas Secretary of State • Virginia ○ Department of Accounts ○ Department of Health ○ Library of Virginia ○ State Corporation Commission ○ Virginia Information Technology Agency ○ Virginia Retirement System • Washington ○ Department of Corrections ○ Department of Ecology ○ Department of Financial Institutions ○ Department of Licensing

Cyber Storm VI Participants
○ Department of Services for the Blind ○ Office of Cyber Security ○ School for the Blind ○ Washington Technology Solutions *Observing States:* • Alabama • Connecticut • Georgia • Hawaii • Idaho • Illinois • Indiana • Massachusetts • New Jersey (participated through Critical Manufacturing Community) • North Carolina • New York • Oregon • Pennsylvania
Industry Entities
• Air Products and Chemicals, Inc. • American Express Global Business Travel • American Honda Motor Co., Inc. • American Outdoor Brands Corporation • Aptiv • AT&T • Atlas Air • BASF Corporation • The Boeing Company • CenturyLink • Charter Communications • Cox Communications • Crowdstrike • Cyxtera • Deere & Company • Dell Secureworks • The Dow Chemical Company • Eli Lilly and Company • Fiat Chrysler Automobiles • Ford Motor Company • General Motors • Geotab • Hyundai America Technical Center Inc. • Hyundai Motor America • Intel • Lear Corporation • Lennox International Inc. • McAfee • Merck & Company, Inc. • Middlesex Water Company

Cyber Storm VI Participants
• Mitsubishi Motors R&D of America, Inc. • National Motor Freight Traffic Association • Navistar, Inc. • Northrop Grumman Corporation • Nucor Corporation • Oshkosh Corporation • Pfizer Inc. • PPG Industries, Inc. • Siemens Corporation • Sprint • T-Mobile • Tower International • Verizon • Verizon Threat Research Advisory Center
Coordination Bodies
• American Chemistry Council (ACC) • Automotive Information Sharing and Analysis Center (Auto-ISAC) • Aviation ISAC (A-ISAC) • Axon Global • Communications Information Sharing and Analysis Center (Comms ISAC) • Cyber Response Group (CRG) • Cyber Threat Alliance • Cyber Unified Coordination Group (UCG) • Global Manufacturing Information Sharing & Analysis Organization (GM-ISAO) • Information Technology ISAC (IT-ISAC) • International Association of Certified ISAOs (IACI) • Manufacturers Alliance for Productivity and Innovation (MAPI) • Multi-State Information Sharing and Analysis Center (MS-ISAC) • National Health Information Sharing and Analysis Center (NH-ISAC) • New Jersey Cybersecurity and Communications Integration Cell (NJCCIC)
International Entities

• Australia
  ○ Computer Emergency Response Team (CERT)-Australia
• Canada
  ○ Canadian Cyber Incident Response Centre (CCIRC)/Public Safety Canada
• France
  ○ National Cybersecurity Agency of France (ANSSI)/CERT-France
• Germany
  ○ Federal Office for Information Security (BSI)/CERT-Bund
• Hungary
  ○ GovCERT-Hungary
• Japan
  ○ Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
  ○ National Center of Incident Readiness and Strategy for Cybersecurity (NISC)
• Netherlands
  ○ National Cyber Security Centre of the Netherlands (NCSC)
• New Zealand
  ○ CERT New Zealand
• Norway
  ○ Norwegian National Security Authority (NSM)/NorCERT

Cyber Storm VI Participants

• Sweden
  ○ Swedish Civil Contingencies Agency (MSB)/CERT-SE
• Switzerland
  ○ Swiss Analysis and Reporting Unit for Information Assurance Operation and Information Centre (MELANI OIC)/SWITCH-CERT
• United Kingdom
  ○ National Cyber Security Center of UK (NCSC-UK)