Cyber incidents are occurring with increasing frequency, and these incidents are becoming more disruptive and costlier to governments, businesses, and individuals. Most of these incidents are addressed through regular coordination and response mechanisms; however, some such incidents exceed stakeholders’

KEY FINDINGS

- Decisionmaking for response to a significant cyber incident affecting a National Critical Function (NCF) is challenging because those events can involve rapidly unfolding incidents, a high degree of uncertainty, an indefinite beginning and end, and an unknown cause.

- Planning is especially critical because government and private-sector responders responsible for NCFs have experienced relatively few significant cyber incidents.

- Contingency plans (CONPLANs) are useful tools to facilitate coordinated, rapid, and effective response to significant cyber incidents and other contingencies.

- Plans help clarify incident response stakeholders’ roles and responsibilities, establish requirements for information-sharing, specify coordination mechanisms, identify possible interdependencies and cascading effects, and identify actions to improve preparedness and resilience in advance of a significant cyber incident.

- The process of developing the plan is just as important as the resulting document. The planning process can illuminate authorities, capabilities, and competencies that are relevant to incident response and deepen stakeholders’ understanding of their respective roles and responsibilities.

- Building the core planning team is critical to the planning process. The team should include a lead entity and representatives of key organizations responsible for NCF cyber incident response.

- The planning process has five steps: Gather data and survey the threats, develop mission statements and objectives, develop courses of action, draft a plan, and evaluate risks to the plan.

- Stakeholders can operationalize an approved CONPLAN by disseminating it; testing, exercising, and training with it; documenting and reviewing lessons learned; developing a knowledge base on cybersecurity and resilience; and maintaining and updating the plan.
capacity to respond using everyday means. U.S. government policy, as stated in PPD-41, defines *significant cyber incident* as

a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. (Obama, 2016)

The stakes are particularly high with respect to U.S. National Critical Functions (NCFs). NCFs are defined as “functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.” Securing NCFs requires not just unity of effort within the U.S. government but also effective collaboration and cooperation within state, local, tribal, and territorial (SLTT) governments and the private sector. As noted in the Cyberspace Solarium Commission report,

Most of the critical infrastructure that drives the American economy, spurs technological innovation, and supports the U.S. military resides in the private sector. If the U.S. government cannot find a way to seamlessly coordinate with the private sector to build a resilient cyber ecosystem, the nation will never be secure. And eventually, a massive cyber attack could lead to large-scale physical destruction, sparking a response of haphazard government overreach that stifles innovation in the digital economy and further erodes American strength.

In response to a significant cyber incident affecting an NCF, private-sector stakeholders, federal agencies, and others, including SLTT governments, have critical competencies, authorities, and capabilities that must be seamlessly coordinated to rapidly and effectively respond to and mitigate disruptions to NCF infrastructure.

Although private-sector and public-sector stakeholders collaborate regularly in response to cyber and other incidents affecting NCFs, response to a *significant* cyber incident requires special coordination mechanisms because of the extensive capabilities and competencies in government and the private sector needed to respond effectively to such incidents. Recognizing this need for enhanced coordination, in 2016, the U.S. government set forth policy (PPD-41) and a high-level plan (the National Cyber Incident Response Plan) to promote unity of effort among federal respondents to such incidents. These documents do not, however, specify private-sector or SLTT stakeholders’ roles and responsibilities in cyber incident response or how all stakeholders’ efforts are to be coordinated in response to significant cyber incidents affecting NCFs.

To address this gap, CISA asked the Homeland Security Operational Analysis Center (HSOAC), a federally funded research and development center operated by the RAND Corporation for DHS, to develop a contingency plan (CONPLAN) to guide the private-sector and federal response to a significant cyber incident affecting one NCF, Operate Core Network. The HSOAC research team developed the CONPLAN in coordination with federal stakeholders and representatives from the communications sector, including the four owners and operators of core networks in the United

---

**Abbreviations**

- **CISA**: Cybersecurity and Infrastructure Security Agency
- **CONPLAN**: contingency plan
- **DHS**: U.S. Department of Homeland Security
- **HSOAC**: Homeland Security Operational Analysis Center
- **NCF**: National Critical Function
- **PPD**: presidential policy directive
- **SLTT**: state, local, tribal, and territorial
The resulting plan can memorialize understandings related to each of these areas, serving as a guide for use during incident response. The process of developing the plan is just as important as the resulting document. The planning process promotes critical thinking about the problem of responding to significant cyber incidents. A rigorous development process will illuminate the authorities, capabilities, and competencies that might be relevant to
incident response and consequence management. Through the planning process, stakeholders can deepen their understanding of their respective roles and responsibilities and can establish expectations for coordination, communication, and information sharing.

**Cyber-Specific Planning Challenges**

Planning is particularly important for cyber incident response because of the decision-making environment in which response takes place (see Table 1):

- Cyber incidents unfold rapidly, which means that there might be limited windows in which to take action to mitigate the impact of an incident.
- Cyber incidents are characterized by a high degree of uncertainty, and responders need to make decisions about response based on imperfect information.
- Unlike other incidents, such as a natural hazard, a cyber incident might not have a defined start and end. Intrusions are often not detected immediately, allowing intruders to gain entry and conduct network reconnaissance without causing immediate damage or harm. It also might be difficult to determine whether or when an incident has concluded and the threat actor has been effectively removed from the system.
- The cause of an incident, including whether it was caused inadvertently or it was caused intentionally by a malicious actor, might not be known.

The environment in which an ongoing cyber incident occurs can impair planners’ ability to coordinate response effectively. The incident might limit planners’ ability to communicate with each other, share information, and mitigate the impacts of the cyber incident because of ongoing adversary activity or the effects of the incident. Uncertainty related to some of the elements of an incident can slow or complicate response. For example, efforts to understand the nature and scope of an incident can siphon attention away from response.

Planning can also be particularly important for response to a significant cyber incident because government and private-sector responders have experienced relatively few such incidents. As a result, incident response capabilities and processes are less tested and refined than for noncyber incidents. In contrast, for example, the electricity industry has experienced decades of severe weather incidents, such as hurricanes, that have informed response efforts at various levels of government and within the industry.

**Levels of Planning**

A plan can be developed at a strategic, operational, or tactical level:

- Strategic-level planning sets the context and expectations for operational planning. A strategic-level plan provides an overarching framework that establishes a foundation for policy, operational planning, and resource decisions.
- Operational-level planning identifies the tasks and resources needed to execute a strategic-level plan. An operational plan describes roles and responsibilities, tasks, coordination and integration of activities and resources across agencies and organizations, and other expectations of participating organizations during actual and potential incidents.
- Tactical-level planning shows how to apply resources to complete the operational tasks within a given time frame. A tactical plan sets forth detailed actions necessary to accomplish goals identified in an operational plan.
In this report and the related how-to guide, we focus on operational-level planning. We do not discuss how to develop a tactical-level plan, but an operational-level plan can serve as the basis for and motivate such planning and can help stakeholders identify needed resources, training, and equipment prior to an actual incident.
Components of an Operational-Level Plan

An operational-level CONPLAN should specify

- the **purpose** of the plan, **objectives** for incident response, and the desired **end state**
- **threats** or **risks** at which the plan is directed
- **scope** of application: the circumstances to which the plan is intended to apply
- conditions that can lead to plan **activation**
- organizational **roles**, **responsibilities**, and **coordination mechanisms**.

In addition, the plan should be clear and specific, logically organized, feasible to execute, sufficiently resourced, and consistent with legal authorities and guidance.

A CONPLAN to guide response to a significant cyber incident affecting an NCF can be implemented alongside other plans, including emergency-response and disaster-response plans and playbooks and business continuity plans that might be related to cyber incidents or intended to address the physical consequences of a cyber attack or other incident. Law enforcement and U.S. Department of Defense plans to respond to an adversary might also be relevant in that information derived from the cyber incident response plan can feed into counterthreat planning and perhaps vice versa.

The Planning Process

In this section, we describe each part of the planning process in more detail.

Form the Core Planning Team

One of the most-important questions for initiating planning is **who** should be included in the core planning team. Team leadership is especially critical: The individuals leading the planning process should possess the appropriate authority, relationships, and resources to bring key stakeholders together to form a core planning team, initiate planning, and promote the plan’s adoption.

The core planning team should also include representatives of key organizations with primary responsibility for NCF incident response, as well as experts with experience and expertise in the operation of the NCF. The core planning team can also include hardware and software vendors, cybersecurity companies, and internet service providers. Individual members of the core planning team should have contributed to past planning efforts, possess an understanding of the technical elements of cyber incident response, and be among those responsible for detecting, evaluating, and monitoring threats as they emerge. They should understand the potential impacts of the loss of system functionality and be able to identify NCF dependencies and cascading impacts. The core planning team should also include members with expertise and experience across multiple sectors, including those responsible for operational liaison during an actual incident. At least some members should have a deep understanding of the legal, policy, and regulatory elements of incident response and be able to facilitate engagement with external partners and the public.

It is important to think broadly about who should be involved in planning: Although having a tight core planning group can be effective, gaining input on the plan from a wide variety of relevant stakeholders is also crucial. These stakeholders might include NCF owners and operators, federal and SLTT organizations not already represented on the team, owners and operators of other NCFs linked to the threatened infrastructure, cybersecurity and threat intelligence companies, and experts in academia, think tanks, and similar centers of excellence.
When selecting opportunities for collaboration, planners should look to organizations that are custom-built for sector expertise and information sharing, such as government coordinating councils, sector coordinating councils, information-sharing and analysis organizations, and trade and industry organizations. In selecting processes to facilitate planning, the team should consider who is available, how much time each participant can contribute to the effort, what opportunities there will be to consult with key constituencies, and any external requirements or deadlines.

In determining the time horizon for the plan, team members must decide how far into the future the plan can be reliably executed. Planners should consider how regularly the plan is tested through structured exercises or other activities, how often it should be circulated to stakeholders for awareness and review, and how often the plan should be formally updated.

Once the core planning team and other stakeholders are in place and approaches for collaboration have been chosen, the team can begin the planning process itself. We have divided this process into five steps, as shown in Figure 1. In this section, we briefly discuss each step in turn.

Gather Data and Survey the Threats

Data gathering orients planners to the problem, provides a starting point for planning, and informs the plan. Planners should try to identify documentation that can help the planning team understand the NCF itself, risks and threats to the NCF, and ways in which NCF stakeholders currently approach incident response. The scope of materials that might be relevant can be quite broad, and planners should err on the side of casting a wide net to ensure that planners are not missing potentially valuable materials. Data gathering can be an iterative process, continuing throughout the planning process as new materials are discovered or planners’ questions lead to more data discovery.

Once a critical mass of data has been collected and curated, the next step is to analyze vulnerabilities and threats to the NCF. Planners might face a challenge in identifying threats to the NCF. Cyber threats are pervasive, but significant impacts on the operations of most NCFs have been rare to date, and it can be a challenge to anticipate the types of threats that can lead to a significant cyber incident. The purpose in planning is not, however, to identify the exact pathway along which a cyber event becomes a significant cyber incident. Rather, planners should focus on the types of significant impacts that might occur and then posit ways in which a cyber incident could cause those impacts—for example, a large cyber attack compromising the generation and transmission of energy, similar to the blackouts that occurred in Ukraine in 2015.\textsuperscript{12}

A cyber incident affecting an NCF or NCFs would likely be complex but will often begin with compromises to business systems and enterprise networks. These incidents can start with an adversary gaining an initial foothold on a network through the business systems—exploiting email server vulnerabilities or compromising a user account that has privileged access, for example—demonstrating that sig-
significant cyber incidents can originate in ways that are difficult to distinguish from more-conventional cyber incidents that organizations face every day.

As planners explore the threat landscape, they will also need to consider the ways in which NCFs relate to each other. Understanding these connections and the potential for cascading effects that can affect multiple NCFs is a critical and challenging component of the planning process.

Once a planning group has gathered materials on threats to the NCF and incident reports, members will want to consider how to prioritize the threats and risks to the NCF. This activity serves two functions: It can inform the development of scenarios for which to plan and can be used to inform risk-mitigation efforts either in parallel with or subsequent to the planning process.

The process of surveying threats requires anticipating what kinds of decisions will need to be made in an incident, what uncertainties should be anticipated, what information will be needed during an incident, and what lessons stakeholders have learned from previous incidents. One especially helpful tool for addressing these issues is the tabletop exercise, which can help the planning team explore the threat space, evaluate courses of action, test the plan, train stakeholders, and allow stakeholders to work with each other before a real incident.

At this point, it is important to identify the methods to be used in developing the plan. There are two primary approaches to contingency planning: scenario-based planning and functional planning. Scenario-based planning, as the name implies, uses a postulated scenario—a description of some adverse event—as the basis for developing an incident response plan. A sufficiently broad array of plausible scenarios will yield a series of plans capable of addressing them. Functional planning, on the other hand, identifies the common functions that must be performed in any incident response (e.g., incident detection and assessment, notification of partners, forensic analysis). In many cases, a hybrid approach consisting of functional planning followed by scenario-based planning could provide the best of both worlds.

Dependencies and Interdependencies Between National Critical Functions

As planners explore the threat landscape, they will need to consider NCF dependencies and interdependencies. A dependency is a one-way relationship between NCFs in which one relies on the other. For example, CISA has identified dependencies between four lifeline functions (transportation, water, energy, and communication) for which “a disruption or loss of one of these functions will directly affect the security and resilience of critical infrastructure within and across numerous sectors.” An interdependency is more specifically a relationship between infrastructures through which the
state of each can “influence or correlate to the state of the other.”

Understanding these connections and the potential for cascading effects that can affect multiple NCFs is a critical and challenging component of the planning process. For example, malware often spreads across sectors, organizations, and NCFs and can have effects well beyond a narrow set of organizations. Understanding how cyber threats can propagate across NCFs and sectors can often be difficult to foresee, which underscores the need to cast a wide net in terms of data gathering that pertains to threats and risks and to consult with a broad set of potential stakeholders and experts.

Prioritizing Threats and Risks to the National Critical Function

Once the planning group has gathered materials on threats to the NCF and incident reports, the group will want to consider prioritizing the threats and risks to the NCF. This serves two functions: It can inform the development of scenarios for which to plan and can be used to inform risk-mitigation efforts either in parallel with or subsequent to the planning process. Incident after-action reports and techniques can also help planners answer such questions as these:

- What kinds of decisions must be made in an incident?
- What uncertainties must be anticipated and considered?
- What information is needed during an incident?
- What lessons can be learned from prior incidents about things that went well and things to avoid?

Develop Mission Statements and Objectives

Next, planners should develop an initial mission statement that can help orient planners to the desired goals of incident response. The mission statement is “the organizational purpose and directed objective that shape actions and activities to be executed.” For a CONPLAN, the mission statement should provide a clear articulation of who is doing what to achieve the overall outcome.

The mission statement is supported by a set of objectives that can be articulated in draft form at the outset of the planning process and refined as planning progresses. For cyber incident response planning, objectives might include such actions as detecting emerging cyber incidents that could significantly affect the NCF or assessing the severity of a cyber incident affecting the NCF.

Although the initial mission statement will orient planners for the work described above, a refined mission statement at the end of the process will capture the lessons learned in the process of planning and will orient those who carry out the plan when it is activated during a real-world contingency.

Develop Courses of Action

The next step in the planning process is to develop alternative courses of action (i.e., sequences of actions that an individual or organization can take to accomplish a given objective). Multiple courses of action can help planners identify alternative ways to address a set of challenges and then evaluate those alternatives to determine the most operationally effective approach, minimizing risk and maximizing the probability of success. Each course of action must specify an incident timeline, key decision points, and operational tasks assigned to specific stakeholder organizations. Each course of action should be suitable to the desired objective, feasible, complete, and acceptable in terms of risk.

The first step in developing a course of action is to lay out an incident timeline that captures when major incident response events will occur. Once the timeline has been devel-
oped, the next step is to identify key decision points. The types of decisions that planners should anticipate occurring during incident response are likely to be similar for most cyber incident CONPLANs at the following decision points: initial incident assessment, plan activation, emergency or disaster declarations, notification requirements (e.g., required reporting to government agencies), convening of enhanced operational coordination bodies (e.g., unified coordination group), mobilization of personnel or reserve capacity, and transition from one phase of the plan to another.

The reason for identifying decision points explicitly and in advance of developing a plan is to determine what inputs decisionmakers will need to inform those decisions, to prepare for how to implement those decisions, and to identify the resources that might be required to support those decisions, which can include personnel, equipment, and infrastructure.

The final step in developing a course of action is to assign operational tasks to stakeholder organizations. These tasks should focus on who is doing what and to what end. Operational tasks should align to a particular stakeholder and identify the nature of the task, who is responsible for executing the task, and any special considerations for the timing or interdependencies of tasks.

After the alternative courses of action have been developed, they must be analyzed, and one must be selected. This analysis might be accomplished through tabletop exercises or a decision matrix. For the latter, planners identify criteria to evaluate each course of action and assign a weight to each criterion depending on its importance. Each course of action should be evaluated on its own merits rather than being compared with the other courses of action. Different approaches can be employed to gather subject-matter expert inputs related to the courses of action, such as the Delphi method—a process of eliciting input from a group of experts, typically via multiple rounds of questionnaires, seeking to arrive at an approximation of a group consensus—or elicitation of advantages and disadvantages from each planner and additional experts.

Identify Key Tasks and Activities, and Draft a Plan

After gathering and analyzing relevant data, deciding on a planning process, crafting an initial mission statement and objectives, and identifying the preferred course of action, planners are prepared to develop the CONPLAN. There are four main components to the CONPLAN:

- **situation**: explains why the plan was developed and provides information on the scope and key assumptions of the plan
- **overview**: describes the mission, objectives, roles, and tasks for the key stakeholders who will execute the plan
- **execution**: describes step by step how stakeholders will respond to a significant cyber incident, including how they will identify and assess incidents (phase 1), coordinate and remediate the incident (phase 2), and mitigate and transition into postincident operations (phase 3), and explains operational coordination and information sharing
- **appendixes**: provide additional information that is self-contained but useful for executing the main plan.

Table 2 provides more information about the contents of each section, which are discussed in detail in the how-to guide. Planners should include all the sections shown in the table in their CONPLANs.

Evaluate Risks to the Plan

Once the plan components have been developed, planners need to evaluate the risks to plan execution and to the supported NCF. The
### TABLE 2
Sections and Contents of a Contingency Plan

<table>
<thead>
<tr>
<th>Section</th>
<th>Goal</th>
<th>Example Contents</th>
</tr>
</thead>
</table>
| Situation | Provide an overarching picture of the CONPLAN and orient CONPLAN users to help them understand how to use the CONPLAN. In this section, planners, define the purpose and scope of the plan, relevant impacts, time period, and response activities that are in scope. | - **Purpose:** addresses the question, “why was this plan developed?”  
  - **Scope:** describes the extent and parameters of the plan  
  - **Background:** describes how the plan relates to related efforts, such as cyber and emergency-response planning activities  
  - **Potential Threats to the NCF:** outlines the threats that, if realized, might necessitate CONPLAN activation  
  - **Planning Assumptions:** explains the assumptions on which the plan is based  
  - **Critical Considerations and Additional Context or Issues:** identifies considerations and issues that can affect plan execution  
  - **Authorities:** outlines the primary sources of legal authority and guidance that pertain to incident response and stakeholders’ roles and responsibilities |
| Overview  | Focus the plan on a mission area and explain what the plan is supposed to cover and who is supposed to use the plan—as well as what the plan does not cover. | - **Mission:** includes the intent of plan stakeholders, overall plan end state, potential metrics  
  - **Objectives:** describes broad goals of the plan  
  - **Roles and Responsibilities:** indicates what key stakeholders will do in each phase of the plan  
  - **Mission-Essential Tasks:** describes the tasks that must be performed to complete the mission |
| Execution | Describe step by step how stakeholders will respond to a significant cyber incident, including how they will identify and assess an incident, coordinate and remediate the incident, and mitigate and transition into postincident operations. Explain operational coordination and information-sharing mechanisms. | - **Concept of Operations:** describes how the public- and private-sector capabilities will be jointly employed and coordinated in the event of a significant cyber incident to achieve the plan’s objectives and includes a high-level statement describing the key stakeholders, how they will collaborate in response to achieve the overarching objective  
  - **Criteria for the Activation of the Plan:** documents the process for activation, including triggers or escalation criteria, as well as related processes  
  - **Plan Phasing:** includes details on the activities NCF stakeholders will execute across the phases of cyber incident response, the capabilities they bring to bear, how they collaborate with other stakeholders, and what support they seek from the federal government  
  - **Operational Control and Information Sharing:** describes the structures, channels, and practices for sharing information across the U.S. government and between the U.S. government and relevant NCF stakeholder entities; describes key federal coordination mechanisms, including the Cyber Response Group and Cyber Unified Coordination Group; and describes the use of information-sharing and analysis centers to share cyber threat information to key stakeholders and best practices for protecting sensitive information |
| Appendixes| Provide additional information that is self-contained and supportive of the main plan. | - **Administration, Resources, and Funding:** provides guidance on mechanisms that can be used during an incident response to document decisions, directions, and actions, and sources of funding that are available to support plan execution when needed  
  - **Cyber Incident Information Elements:** provides the CISA template for identifying cyber incident information elements and explains why having a consistent way of collecting and communicating these elements will aid NCF stakeholder engagement with the government  
  - **Mutual-Aid Processes:** discusses the nature of cyber mutual-aid mechanisms, resources, or other assistance that NCF stakeholders might provide to one another during response  
  - **Key Terms:** provides a limited list of key definitions focusing on terms that are not used in a standard way  
  - **Points of Contact:** identifies key points of contact for NCF and federal stakeholders  
  - **Other Checklists and Standard Operating Procedures:** includes example checklists or procedures to help incident responders quickly follow the CONPLAN and ensure that no key steps are missed in the response process |
objective of the CONPLAN is to mobilize and coordinate resources and capabilities in time and space to respond to, contain the effects of, and mitigate the consequences of a significant cyber incident and establish the conditions for long-term recovery. Therefore, the risk assessment should focus on risks that, if realized, could compromise the ability to successfully execute the CONPLAN, resulting in delays in providing adequate response to a significant cyber incident; such risks could include challenges in timely identification of a significant cyber incident, inability to access necessary response resources, or problems with information sharing. There are two broad categories of these types of risk:

- risks that might inhibit the successful resolution of the significant cyber incident for the NCF executing the CONPLAN
- risks that, if realized as part of executing the CONPLAN, could compromise other NCFs’ ability to provide essential services.

Both these categories of risks need to be identified, assessed, and remediated in the risk-assessment process as part of developing a successful CONPLAN.

Figure 2 shows the three main steps involved in evaluating risk to the CONPLAN.

Risk identification involves the generation of a large list of risks. This list might be developed through group interviews, focus group discussions, or individual interviews with knowledgeable stakeholders and subject-matter experts. Risk analysis involves developing a sense of the likelihood and consequence of different risks, thus discerning which risks might be significant and the focus of remediations. These analyses can be based on qualitative assessments, such as expert evaluation, and quantitative analysis that assigns probabilities and impacts. Risk reduction can be accomplished in many ways, such as by strengthening protections designed to prevent cyber attacks from creating critical cascading failures; improving the identification of emerging threats to reduce delays in response via enhanced risk assessment and information sharing; or prepositioning stocks and resources and conducting regular training and exercises to ensure that plans are properly resourced and personnel are ready.

Reducing risk can be a resource-intensive endeavor, so high-likelihood and -consequence risks should be prioritized for remediation, while low-consequence and -likelihood risks might not be remediated. Medium risks—those with either low likelihood and high consequence or high consequence and low priority—are both of roughly equal importance. The specific remediation plans are contingent on stakeholder capacity: Different stakeholders will have different roles and responsibilities for remediation based on their missions and mandates and the economic, political, and social resources at their disposal. Given capacity differences, the general process for remediation planning is as follows:

1. Brainstorm what can be done.
2. Discuss the utility of these measures for reducing risk and ease of implementation of each measure.
After the plan is developed, it is important to develop a process to ensure that the plan is maintained in a state of readiness, reflects emerging cybersecurity risks, and informs actions that stakeholders should take to improve their response capabilities.

3. Develop specific, measurable, achievable, relevant, time-bound plans for promising remediation interventions.

Risk remediations can involve either changing the contents of the CONPLAN itself (such as by modifying response procedures to reduce reliance on a set of resources that might not be available) or taking additional action outside of the CONPLAN (such as by improving the reliability of those resources).

**Operationalizing the Plan**

A CONPLAN should be viewed as a starting point that encourages stakeholders to think critically about how to respond to a significant cyber incident and develop the capabilities required to do so effectively. Thus, after the plan is developed, it is important to develop a process to ensure that the plan is maintained in a state of readiness, reflects emerging cybersecurity risks, and informs actions that stakeholders should take to improve their response capabilities. In this section, we highlight some ways in which the plan can be operationalized.

**Disseminate the Plan**

Once the plan is complete, planners should ensure that it gets to the people and organizations who will use it in an emergency. Planners should ask, “Who should have this plan ready to use on their shelf?” and consider disseminating the plan to stakeholders who were identified during the planning process. The dissemination process should be viewed as an opportunity to reinforce the planning principles outlined in the document, encourage stakeholders to use the plan to strengthen their response capabilities and inform internal response plans, and raise awareness of the plan among stakeholders who did not directly participate in its creation.

When appropriate, planners should offer to have follow-up discussions or briefings with those parties with whom the plan is shared to discuss its purpose and request feedback on its contents. Planners might want to consider designating a steering committee or postplanning coordinator from among NCF stakeholders to maintain the plan as a living document, collect feedback and suggestions for revisions, inform stakeholders of proposed revisions, and develop and carry out a process to update the document based on identified events or triggers.

**Test, Exercise, and Train with the Plan**

Tests and exercises are important tools for organizations to use in validating the plan, identifying gaps and weaknesses, and informing remedies. Organizations can use tests or
operations-based exercises to validate or “stress-test” the plan and identify gaps and limitations in response capabilities. The National Institute of Standards and Technology recommends conducting tests in an operational environment that is as close to a real-world situation as possible and could include introducing failure to components or systems used for operations. Alternatively, organizations can use discussion- or operations-based exercises as educational tools to strengthen stakeholders’ capabilities and improve participants’ familiarity with plan contents and tasks. Functional exercises, by contrast, can be conducted in a simulated operational environment rather than a classroom or virtual setting and seek to validate an organization’s operational readiness.

Many cyber incidents will require stakeholders to conduct activities that differ considerably from their typical duties. They also require some response personnel to possess specialized knowledge and skills in technical areas, such as intrusion detection and forensics. As a result, organizations should develop training programs to help ensure that the various personnel involved in the CONPLAN response understand the roles and responsibilities assigned to them and are fully equipped to carry them out effectively. Such activities can take many forms, including instructor-led training in a classroom, interactive online, or self-study. Each organization should identify the training curriculum that best prepares its personnel, given any unique considerations that might apply to them.

To support stakeholders’ training objectives, CISA has developed no-cost cybersecurity incident response training for government employees and contractors across federal and SLTT entities, which is also available to educational and critical infrastructure partners. The curriculum provides a variety of offerings for beginner, intermediate, and advanced cyber professionals, including “basic cybersecurity awareness and best practices for organizations, live red/blue team network defense demonstrations emulating real-time incident response scenarios, and hands-on cyber range training courses for incident response practitioners.”

Stakeholders might also consult the National Institute of Standards and Technology’s Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, which provides detailed guidelines on designing, developing, conducting, and evaluating tests, training, and exercises. In particular, the guide outlines a common method for developing test, training, and exercise programs to offer organizations different ways of identifying and addressing gaps and limitations in response plans and to ensure that such events are performed as consistently and effectively as possible while reducing duplication of effort.

Document and Review Lessons Learned

Organizations can benefit from a lessons-learned process to collect insights from real-world cyber incident responses, as well as tests and exercises, and adjust plans for future use. Each organization should consider developing a rigorous after-action review process to document and review past cyber incidents affecting its sector or NCF and evaluate whether established procedures outlined in the CONPLAN were followed and whether response actions taken were effective and to identify lessons to inform revisions to the plan, training, or improvements to capabilities. Such postincident analysis can help an organization understand what went well so that these steps can be codified for future practice and can help planners identify weak points or gaps in the organization’s or its sector’s response plans and help them translate lessons learned into remedial actions. Such analyses, often compiled in after-action reviews, can also help an organization or sector improve its cybersecurity preparedness by providing reference materials in
the event that stakeholders encounter a similar incident in the future. An organization might also consider evaluating its performance during specific aspects of the plan.

**Develop a Knowledge Base on Cybersecurity and Resilience**

Organizations should strive to stay informed of emerging literature and best practices for cybersecurity and resilience that can help them improve their plans. This should include continuously reviewing cybersecurity publications, reports, and trend and threat analyses on significant incidents, as well as participating in information-sharing events, symposia, and informal discussions among sector and NCF communities of interest. Examples include InfraGard events and CISA-hosted events held virtually or in person around the country. Stakeholders can also participate in cross-sector crisis-management and contingency planning exercises to stay informed of emerging literature and approaches for improving response to cyber incident with systemic impacts. Information and knowledge learned from such efforts could lead stakeholders to reconsider key assumptions or approaches that were central to the planning process—such as new cyber risk-management best practices or evolving regulatory, legal, and business requirements—and could prompt sectors to revise elements of the plan.

**Maintain and Update the Plan**

To be effective, the response plan should be a living document that is revised regularly to reflect changes in issues that are important to its development, such as organizational structures and authorities, cybersecurity risks, and policy guidance. Plan stakeholders should develop a monitoring process to ensure that the plan is regularly reviewed for accuracy and completeness and that the response capabilities on which the plan relies are maintained at a state of readiness. Ideally, stakeholders should identify both the mechanism by which they will trigger plan revisions as part of finalizing the plan and at least one organization or point of contact (with a backup) to serve as the plan “custodian” to maintain authoritative copies of the plan and register changes over time. The frequency of monitoring should be defined by key stakeholders and can be time-based (e.g., annually) or triggered by significant changes to key elements that inform the plan.

Each stakeholder organization should also determine the resources required to maintain the plan and identify resources to meet the objectives specified in the plan. Resources should be sufficient to conduct activities necessary to the plan maintenance, such as to conduct cross-sector testing, training, exercises, and other events. Resources are not just financial but also include staff time and availability to focus on these activities.

**Conclusion**

Developing a response plan for significant cyber incidents is a complex undertaking requiring close collaboration across multiple stakeholders. The how-to guide developed by HSOAC researchers and CISA personnel, *Planning for Significant Cyber Incidents: Cyber Incident Contingency Planning How-To Guide*, provides a step-by-step framework for developing
an effective plan, including a robust template plan, that can be used by NCF stakeholders to develop plans for their sectors and NCFs.\textsuperscript{24}

As planners and other stakeholders undertake these planning efforts, they are encouraged to share lessons learned and insights with CISA to inform its support to contingency planning.

Notes

1 Per Presidential Policy Directive (PPD) 41, “United States Cyber Incident Coordination,” a cyber incident is

\[\text{an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. (Obama, 2016)}\]

See, e.g., Welburn and Strong, 2021: “Cyber incidents have risen both in prevalence and significance in their disruptions to individuals, businesses, and governments” (p. 1). See also U.S. Government Accountability Office, 2020:

\[\text{Cyber-based intrusions and attacks on both federal and nonfederal systems have become not only more numerous and diverse, but also more damaging and disruptive. Moreover, the risks to systems supporting the federal government and the nation’s critical infrastructure are increasing. (p. 1)}\]

2 See also Boyd, Kuldell, and Jasper, 2020.

3 See Cybersecurity and Infrastructure Security Agency (CISA), undated c. In April 2019, CISA published a set of 55 NCFs (CISA, 2019a). In July 2020, CISA published a status update that included definitions of each of these 55 NCFs (CISA, 2020).

4 Cyberspace Solarium Commission, 2020, p. 7.

5 This report uses the phrase \textit{incident response} to include the full span of activities that could occur, from incident identification, plan activation, incident remediation activities and coordination, mitigation, and transition to postincident operations. This includes analysis to understand the incident, its cause and impacts, technical recovery actions, communications and reporting, and coordination between stakeholders engaged in response.

Some guidance related to incident response distinguishes between \textit{incident management}, efforts to organize the response, including logistics and coordinating resources, and \textit{incident response}, which includes technical recovery actions and other response activities (see National Cyber Security Centre, 2019). The how-to guide does not make this distinction and includes efforts to organize the response within the broader category of \textit{incident response}.


7 Kotila et al., 2021.

8 The cybersecurity firm CrowdStrike estimated that the average “dwell time” for an adversary on a network before detection was 95 days in 2019; see Mallon, 2020.

9 For example, after Hurricane Sandy, a well-established network of mutual-assistance programs enabled the proliferation of resources to swiftly restore power to those who needed it. See Stockton, 2016, pp. 1–3.
For example, energy stakeholders provide essential power and fuels to stakeholders in the communication, transportation, and water sectors, and, in return, the energy sector relies on them for fuel delivery (transportation), electricity generation (water for production and cooling), as well as control and operation of infrastructure (communication). These connections and interdependencies between infrastructure elements and sectors mean that the loss of one or more lifeline function(s) typically has an immediate impact on the operation or mission in multiple sectors. (CISA and Bureau of Counterterrorism, 2019, p. 4)


For cyber incidents, this might include sets of similar stakeholders, such as owners and operators of NCF systems and networks.

Crolee Dalkey and Helmer-Hirschberg, 1962.

See CISA, undated b.
References


CISA—See Cybersecurity and Infrastructure Security Agency.

CISA and Bureau of Counterterrorism—See Cybersecurity and Infrastructure Security Agency and Bureau of Counterterrorism.


FEMA—See Federal Emergency Management Agency.


InfraGard, homepage, undated a. As of September 15, 2021: https://www.infragard.org/

———, “InfraGard Program Calendar,” webpage, undated b. As of September 15, 2021: https://www.infragard.org/Application/General/Events


PPD-41—See Obama, 2016.


About This Report

This report is intended to help National Critical Function (NCF) stakeholder organizations, which can include private-sector entities and federal, state, local, tribal, and territorial governments, prepare to develop contingency plans (CONPLANs) to respond to and mitigate the impacts of a significant cyber incident affecting their NCFs. It summarizes key elements of a contingency planning how-to guide developed by experts from the Homeland Security Operational Analysis Center (HSOAC) and the Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security (DHS). That guide provides a CONPLAN template and sets forth a process, questions, and considerations for stakeholders to consider in developing an NCF CONPLAN. This report is not intended to describe in detail all of the steps involved in developing and disseminating a CONPLAN; we refer the reader to the guide for that information. Instead, it summarizes the major concepts that are explored in detail in the full how-to guide.

This report should be of interest to leaders and managers in NCF stakeholder organizations and other entities that have a role in cyber incident response. The companion how-to guide will be relevant for NCF stakeholders who seek to develop NCF-specific cyber incident CONPLANs. A stakeholder that wishes to develop an NCF-specific CONPLAN can leverage individual sections of the how-to guide or the entire how-to guide, depending on the maturity of the stakeholder’s existing planning capabilities and processes. The stakeholder can use the CONPLAN template as a starting point for the planning process or start from a blank file, using the how-to guide as a reference.

This research was sponsored by CISA and conducted within the Strategy, Policy, and Operations Program of the HSOAC federally funded research and development center.