A picture containing outdoor, building, government building

Description automatically generated

**CISA Tabletop Exercise Package**

**Federal Civilian Executive Branch Distributed Denial of Service**

[Enter Organization Name]

## <Insert Date>

## Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc143606182)

[Exercise Overview 5](#_Toc143606188)

[General Information 6](#_Toc143606189)

[Module 1 8](#_Toc143606190)

[Module 2 10](#_Toc143606191)

[Appendix A: Additional Discussion Questions 12](#_Toc143606192)

[Appendix B: Acronyms 16](#_Toc143606193)

[Appendix C: Case Studies 17](#_Toc143606194)

[Appendix D: Attacks and Threats 18](#_Toc143606195)

[Appendix E: Contacts and Resources 19](#_Toc143606196)

# Handling Instructions

**Delete instructions that are not applicable.**

TLP:CLEAR

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):CLEAR*”: Recipients can spread this to the world; there is no limit on disclosure. This designation is used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:GREEN

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):GREEN*”: Limited disclosure, recipients can spread this within their community. This designation is used when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. **Note: When “community” is not defined, assume the cybersecurity/cyber defense community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):AMBER”:* Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER+STRICT

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *“Traffic Light Protocol (TLP):AMBER+STRICT*: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Note that “*TLP:AMBER+STRICT”* restricts sharing to the organization only. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TLP:AMBER+STRICT information with members of their own organization, but only on a need-to-know basis to protect their organization and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER+STRICT and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:RED

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):RED*”: For the eyes and ears of individual recipients only, no further disclosure. This designation is used when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

# 

# Exercise Overview

|  |  |  |
| --- | --- | --- |
| Exercise Name | Exercise Name | |
| Exercise Date, Time, and Location | Exercise Date  Time (e.g., 9:00 a.m. – 12:00 p.m.)  Exercise Location | |
| Exercise Activities | Time | Activity |
| 20 Minutes | Threat Briefing and Opening Remarks |
| 60 Minutes | Module 1 |
| 20 Minutes | Break |
| 60 Minutes | Module 2 |
| 20 Minutes | Hotwash |
| Purpose | Examine the cyber resilience of <federal agency> in response to a Distributed Denial of Service (DDoS) incident. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Examine <federal agency>’s ability to detect and respond to a DDoS attack. 2. Discuss <federal agency>’s information sharing protocols with internal and external stakeholders/partners. 3. Review <federal agency>’s reporting protocols to meet Federal Incident Notification Guidelines. 4. Discuss <federal agency>’s plans to restore capabilities/services impacted by a cyber incident. | |
| Threat or Hazard | Distributed Denial of Service | |
| Scenario | A cyber threat actor launches a DDoS attack against Federal Civilian Executive Branch (FCEB) agencies, overwhelming servers. | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program (NCEP)**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov) | | |

# General Information

## Building Resilience

The purpose of the National Cyber Exercise Program’s CISA Tabletop Exercise Packages (CTEPs) is to increase your organization’s resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”[[1]](#footnote-2)

## Using this Situation Manual

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. There are footnotes with corresponding resources throughout the modules to guide your preparedness efforts. The appendices provide the following information to tailor the exercise discussion:

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions
* Appendix B: Reference section for acronyms used within this situation manual
* Appendix C: Case studies that provide real-world examples of the threats presented in this scenario
* Appendix D: An explanation of the threats presented in this scenario
* Appendix E: Additional cybersecurity preparedness and response resources

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario. Players may include IT/information security staff and emergency management staff.

**Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise. Observers may include senior-level staff such as administrators and principals.

**Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.

**Note-takers** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

## Exercise Structure

This exercise is intended to be a multimedia, facilitated exercise. Players will participate in the following:

* Cyber threat briefing (if desired)
* Scenario modules:
  + **Module** **1:** This module addresses the actions your agency takes upon receiving a CISA DDoS Advisory and examines your agency’s baseline planning efforts.
  + **Module 2:** This module explores how your organization handles indicators of a DDoS attack, confirmation of an attack, mitigation, and monitoring and recovery efforts.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Additional discussion questions for each module can be found in Appendix A.*

## Exercise Guidelines

* This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
* Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable insights derived from your training and experience.
* Decisions are not precedent-setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
* There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
* In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

## Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

# Module 1

### Day 1

CISA releases a Federal Civilian Executive Branch (FCEB) Advisory[[2]](#footnote-3) describing increased distributed denial-of-service (DDoS) activity targeting both U.S. and foreign government entities. Recent activity by known cyber threat actors indicate additional planned attacks targeting U.S. infrastructure including airports and weather monitoring centers.

### Day 3

Your agency <insert leadership title> requests a briefing regarding your agency’s actions to protect against, detect, identify, respond to, and recover from a DDoS attack. The tasker specifically requests to know how the agency is addressing the recommendations in the Advisory, as well as the results and lessons learned from your most recent test and/or exercise of the agency’s cybersecurity incident response plan (CIRP)/DDoS response plan.

## Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired. Additional questions can be found in Appendix A.

1. What cybersecurity threat information does your organization receive?
   1. Who within your organization receives it?
   2. What cyber threat information is most useful?
   3. How is information disseminated to the relevant parties within your organization? Externally?
   4. What actions would your organization take in response to an advisory like the one presented in the scenario?
2. What DDoS protections are included in your Terms of Service ageements with your outsourced service providers, such as your Internet Service Provider (ISP), Managed Service Provider (MSP), or Cloud Service Provider (CSP)?
   1. What additional protection against DDoS attacks might your agency consider?
   2. What gaps or limitations in coverage exist?
3. What automated and manual methods of DDoS attack detection and mitigation has your agency implemented?
   1. Who in your agency is notified by the automated detection tools?
   2. How would your agency manually detect a DDoS attack?
   3. How often are these systems tested?
4. What edge network defenses has your agency acquired to reduce the risk of malicious traffic reaching its target while still allowing legitimate users to reach agency services?
5. What is the process to ensure any reporting required by the Federal Information Security Modernization Act (FISMA) occurs as needed?
6. Has your agency incorporated DDoS attack response into your CIRP?
   1. How does your agency identify the type of DDoS attack? Is it documented in your plan?
   2. How does your agency respond to and rapidly recover from DDoS attacks?
   3. How are key personnel trained on roles and responsibilities during a DDoS attack?
7. Has your agency exercised its CIRP against a DDoS attack?
   1. What lessons learned or areas for improvement have you identified?
   2. If lessons learned or areas for improvement were identified, were actions taken to correct or improve the CIRP?

Module 2

### Day 24 – Morning

Your agency’s primary public-facing website, which receives significant daily traffic, is unavailable. Your customer service center receives calls from <customers and/or stakeholders> who cannot access <their accounts/services> via the agency website. They report receiving a “page not found” message when attempting to login.

### Day 24 – Early Afternoon

Network monitoring tools indicate irregular patterns of incoming traffic. Additionally, your outsourced <ISP, MSP, CSP> provider confirms the indications of a DDoS attack.[[3]](#footnote-4)

### Day 24 – Late Afternoon

Your agency’s Security Operations Center (SOC) determines the type of increased traffic against specific system components such as <application layer, protocol, or volumetric attack (select one or more)> was used to disable access to the agency’s websites.[[4]](#footnote-5)

## Discussion Questions

1. What happens when the IT helpdesk receives an increase in similar calls?
   1. How does the helpdesk know there may be a bigger issue?
   2. What are the processes for notifying and/or escalating this issue?
2. What happens when the public facing customer service call center receives an influx of similar calls?
   1. How does the customer service call center know there may be a bigger issue?
   2. What are the processes for notifying and/or escalating this issue?
   3. How does your agency aggregate network disruptions from the IT helpdesk and customer service call center?
3. How does your agency confirm it is experiencing a DDoS attack?
   1. What steps would your agency take once the DDoS attack is confirmed?
   2. How would your agency determine the type of DDoS attack?
   3. Describe how the cascading effects of the DDoS attack will be mitigated.
4. What additional DDoS-specific actions are included in your CIRP?
   1. Who implements these actions?
5. How does your agency continue monitoring and mitigating other cyber-attack vectors during a DDoS attack?
   1. What technical and personnel resources are available to continue monitoring and mitigating against other attack vectors?
6. Who do you notify internally and externally?
   1. Describe the federal notification requirements and process upon confirmation of the incident.
   2. How does your agency notify upstream service providers you are experiencing a DDoS attack?
7. Are there additional capabilities your agency requires?
   1. If your agency relies on another agency, is there a Memorandum of Understanding/ Memorandum of Agreement (MOU/MOA) in place?
   2. If your agency relies on a third-party vendor, are contracts and activation processes in place? Are they tested?
8. How does the reduced staffing around the holiday impact agency response efforts?
   1. How does your organization overcome any staffing deficiencies?
   2. Describe agency contingency plans to address surge staffing requirements.
9. How and when will your agency transition to the recovery and post-incident phases?
   1. How is the decision to transition to the recovery phase made?
   2. How is incident recovery status communicated to internal and external partners and/or stakeholders?
   3. How does your agency conduct post-incident review?
   4. How are lessons learned/areas for improvement incorporated into the agency’s continuous improvement planning?
10. Based on discussion, what changes would you implement to increase the resilience of your organization against future DDoS attacks?

# Appendix A: Additional Discussion Questions

The following section includes supplemental organizational resilience discussion questions designed to guide exercise play. Questions are aligned with the NIST functional areas and organizational roles and responsibilities. Exercise planners are encouraged to select additional, applicable discussion questions for the chosen scenario to bolster participant conversation. *This instructional page, as well as undesired discussion questions, should be deleted.*

## Cyber Resilience

1. Discuss how cyber preparedness is integrated with your current all-hazards preparedness efforts.
2. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
   1. What were the most recent results and action items that followed?
3. Describe your agency’s review process for your CIRP.
4. How often is the CIRP reviewed?
5. Which individual(s) and organization(s) are responsible for reviewing and updating the plan?
6. How are updates to the plan communicated to agency employees?
7. Discuss your supply chain concerns related to cybersecurity infrastructure.
8. What cybersecurity language is included within third-party vendor contracts?
9. How do you evaluate the cybersecurity posture of your vendors?
10. How often are contracts reviewed?
11. How do your service level agreements address cyber incident notification?
12. What level of access do your third-party vendors have to your organization’s network?
13. What is your method for tracking and identifying firmware vulnerabilities in your organization’s network?
14. How are IT and continuity functions coordinated with those responsible for physical security?
15. How is the integrity of your critical data protected and validated?
16. What external entities have access to the database?
17. How would those entities report a breach of their systems to your office?
18. What is your cyber incident management structure?
19. Who leads incident management?
20. How are they notified?
21. How often are roles and responsibilities within this structure exercised with employees?
22. What mission essential functions are impacted by the incidents described in the scenario?
23. How does your organization maintain availability of key assets (e.g., network connectivity, etc.)?
24. If primary communications are compromised, how do you provide information to internal and external entities?
25. What policies and procedures does your agency use to decide when and how to restore backed-up data?
    1. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?

## Employee Accounts & Privileges

1. Describe your agency’s bring your own device (BYOD) policy.
2. What are your agency’s policies or procedures for IT account management?
3. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?

## Incident Identification

1. How does your agency identify all services exposed to the public internet and the vulnerabilities to each of those services?
2. What cybersecurity incident escalation criteria are defined in your cyber incident response plan?
3. Who is responsible and what actions would they take based on the scenario?
4. Who needs to be notified internally and externally according to the plan?
5. When is leadership notified?
6. Discuss your agency’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
7. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
8. How often is your agency’s data reviewed? How do determine whether unauthorized manipulation of data has occurred?

## Incident Response

1. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
   1. How do you capture and share relevant log data and threat indicators?
   2. What type of digital forensics collection capabilities does your agency have in place?
2. What additional concerns have the incidents described in this scenario generated that have not been addressed in today’s discussion?
3. At what point in the scenario would you contact CISA?
4. How does an investigation impact containment, eradication, and recovery efforts?
5. What are the roles of your network operations center and security operations center during a response?
6. What are the processes for contacting critical personnel outside of core hours?
7. How do you proceed if critical personnel are unreachable or unavailable?
8. How would a breach of <entity> affect your agency if they have access to your information?
9. What are the notification requirements to your agency for breaches?
10. Who is responsible for coordinating information across different organizational-level incidents?

## Recovery

1. When does your organization determine a cyber incident is over?
2. Who makes this decision?
3. What post-incident activities would your organization conduct?
4. What actions does your organization take if your IT/incident response staff cannot confirm the integrity of your systems/data?
5. What is the risk associated with re-activating critical business processes and systems?
6. How long and costly is the process to completely rebuild these systems?
7. What factors do you consider when making these decisions?

## Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
2. What additional training and/or exercise requirements do you require for your incident response staff?
3. How often does your organization exercise its CIRP?
4. What agencies are involved in the exercise?
5. What level of the organization is required to participate?
6. How does your organization’s training and exercise efforts address both physical and cyber risks?
   1. Have senior staff participated in a cybersecurity exercise?

## Senior Leaders

1. As a leader in your organization, what cybersecurity resilience goals have you set?
2. How do these goals align with organizational objectives?
3. What cybersecurity training is required for senior leadership?
4. What is your role during a cyber incident?
5. What information do you need to support your decision-making process?
6. What are the gaps in your cybersecurity workforce?
7. How does your organization recruit, develop, and retain cybersecurity staff?

## Public Information

* + - 1. What information are you sharing internally (e.g., employees, leadership)?
      2. What information are you sharing externally (e.g., the public, customers, vendors)?
      3. What training are employees given on reporting any contact with the media to the appropriate public information personnel?
      4. How do you build and maintain trust with the public?
      5. Describe your agency’s reporting and notification requirements.
  1. How does your agency differentiate between an incident and a major incident?
  2. How does the notification requirement for your agency differ between the two?
  3. What timeframes are involved for reports/notifications?
  4. What information must be included in the reports/notifications?
  5. What additional reporting is required for your agency, other than CISA and the Office of Management and Budget (OMB)?

## Legal

1. What is the role of the <Office of the Chief Counsel, Office of the General Counsel> during a cyber incident?
2. What issues need to be addressed based on the scenario?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| APT | Advanced Persistent Threat |
| BYOD | Bring Your Own Device |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| CSP | Cloud Service Provider |
| DDoS | Distributed Denial of Service |
| FBI | Federal Bureau of Investigation |
| FCEB | Federal Civilian Executive Branch |
| FISMA | Federal Information Security Modernization Act |
| ISP | Internet Service Provider |
| IT | Information Technology |
| LL | Lessons Learned |
| MSP | Managed Service Provider |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| POC | Point of Contact |
| SOC | Security Operations Center |
| TLP | Traffic Light Protocol |

# Appendix C: Case Studies

## Coordinated DDoS Attacks on U.S. Infrastructure and Government Websites

The pro-Russian hacktivist group “KillNet” claimed responsibility for large-scale DDoS attacks against websites for the Library of Congress, state governments, and airports nationwide in 2022. The timeline of attacks is below.

Thursday, July 7, 2022, 9:00 p.m.

Access to “Congress.gov” managed by the Library of Congress was unavailable for approximately two hours. The Library of Congress minimized down time by leveraging existing measures to mitigate the attack. The network was not compromised, and no data was lost as a result of the attack.[[5]](#footnote-6)

Wednesday, October 5, 2022

Public facing state government websites in Colorado, Connecticut, Kentucky, and Mississippi were disrupted by a large-scale coordinated DDoS attack. Some of the sites were restored by that afternoon. Colorado’s website was restored the next day. Critical public services were still online and available during the website outages.[[6]](#footnote-7)

Monday, October 10, 2022

The public facing websites for U.S. airports were disrupted by a large-scale DDoS attack. The DDoS attacks overwhelmed the servers hosting these sites with fake requests, making it impossible for legitimate requests from travelers to connect and get updates about their scheduled flights or book airport services. In some instances, the websites became completely inaccessible and in other cases, the connections were extremely slow. The DDoS attack did not directly impact flights.[[7]](#footnote-8)

# Appendix D: Attacks and Threats

## Distributed Denial of Service

Distributed Denial of Service (DDoS) attacks overload bandwidth and connection limits of hosts or networking equipment, specifically through a network of devices (e.g., computers, cellphones, Internet of Things, etc.) making excessive connection requests. DDoS attacks unfold in stages. First, a malicious actor infects a computer with malware that spreads across a network. This infected computer is known as the “master” because it controls any subsequent devices that become infected. The other infected devices, known as “bots” or “zombies” carry out the actual attack and create what is known as a “botnet”. The “bots” receive a command from the “master” which includes the address of the target. Extremely high volumes (floods) of data are sent to the target which slows down web server performance and prevents acceptance of legitimate network traffic. The cost of a DDoS attack can be severe loss of revenue or reputation to the victim.

More information on DDoS attack possibilities within each layer of the Open Systems Interconnection (OSI) Model, as well as traffic types and mitigation strategies, can be found in the resource list below.

### Additional Resources

* Understanding and Responding to Distributed Denial-of-Service Attacks

<https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf>

* Additional DDoS Guidance for Federal Agencies Capacity Enhancement Guide <https://www.cisa.gov/sites/default/files/publications/ceg-additional-ddos-guidance-for-federal-agencies_508c.pdf>
* Understanding Denial-of-Service Attacks <https://www.cisa.gov/news-events/news/understanding-denial-service-attacks>
* DDoS Quick Guide <https://www.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf>
* CISA Alert: DoS and DDoS Attacks against Multiple Sectors <https://www.cisa.gov/news-events/alerts/2023/06/30/dos-and-ddos-attacks-against-multiple-sectors>
* CISA Alert: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>
* MITRE ATT&CK® Network Denial of Service, Technique T1498 – Enterprise <https://attack.mitre.org/techniques/T1498/>
* NIST SP 800-189, Resilient Interdomain Traffic Exchange <https://csrc.nist.gov/publications/detail/sp/800-189/final>

# Appendix E: Contacts and Resources

Federal Government Resources

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
* United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact: <https://www.secretservice.gov/contact/field-offices>, <https://www.secretservice.gov/investigation/cyber>)
* Federal Bureau of Investigation (FBI)
* Field Office Cyber Task Forces (contact: <https://www.fbi.gov/contact-us/field-offices>)
* Internet Crime Complain Center (IC3) (contact: [http://www.ic3.gov](http://www.ic3.gov/))
* National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov); 855-292-3937)
* CISA Federal Government Cybersecurity Incident and Vulnerability Response Playbooks (<https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks>)

1. “Computer Security Resource Center Glossary: Cyber Resilience,” National Institute of Standards and Technology, accessed August 2, 2023, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-2)
2. NIST CSF Tools, “Security Alerts, Advisories, and Directives,” <https://csf.tools/reference/nist-sp-800-53/r5/si/si-5/> [↑](#footnote-ref-3)
3. CISA CPG "Supply Chain Incident Reporting (1.G)" <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals> [↑](#footnote-ref-4)
4. CISA CPG “Detecting Relevant Threats and TTPs (3.A),” <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals> [↑](#footnote-ref-5)
5. A.J. Vicens, “Pro-Russian cybercriminals briefly DDoS Congress.gov*,”* July 8, 2022, *CyberScoop*, <https://www.cyberscoop.com/killnet-congress-ddos-russia-hacktivist/>. [↑](#footnote-ref-6)
6. S. Lyngaas, “Russian-speaking hackers knock US State government websites offline,” *CNN*, October 8, 2022, <https://www.cnn.com/2022/10/05/politics/russian-hackers-state-government-websites/index.html>. [↑](#footnote-ref-7)
7. B. Toulas, “US airports’ sites taken down in DDoS attacks by pro-Russian hackers*,” BleepingComputer*, October 10, 2022, <https://www.bleepingcomputer.com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers/>. [↑](#footnote-ref-8)