# [Enter Organization Name]

## CISA Tabletop Exercise Package

## Federal Civilian Executive Branch Distributed Denial of Service

<Exercise Date>

<Exercise Title>
Situation Manual

## Table of Contents

# 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<br>Time (e.g., 9:00 a.m. – 12:00 p.m.)<br>Exercise Location | |
| Exercise Schedule | **Time** | **Activity** |
| | Time | Activity |
| | Time | Activity |
| | Time | Activity |
| | Time | Activity |
| | Time | Activity |
| | Time | Activity |
| Scope | X hour facilitated, discussion-based tabletop exercise. | |
| Purpose | Examine <insert your agency>'s preparedness to protect against, identify, detect, respond to, and recover from a disruptive Distributed Denial of Service (DDoS) attack. | |
| INSERT: <NIST, FEMA, or Mission Capabilities> | For example, areas such as Identify, Protect, Respond, etc. | |
| Objectives | 1. Examine <insert your agency>'s preparedness to protect the agency from a DDoS attack.<br>2. Examine <insert agency name>'s information sharing protocols with internal and external stakeholders and partners, including commercial service providers.<br>3. Assess <insert your agency>'s plan to detect, respond to and recover from a DDoS attack.<br>4. Review <insert your agency>'s reporting protocols to meet Federal Incident Notification Guidelines.<br>5. Assess <insert your agency>'s communications plan to respond to inquiries from the public and media regarding a DDoS attack. | |
| Threat or Hazard | Cyber | |
| Scenario | A <hacktivist, Advanced Persistent Threat (APT) or criminal (select one)> group with ties to a nation-state 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., Security Operations Center, External Affairs, etc.). | |
| Points of Contact | **Insert Organization POC(s)**<br>Contact info | **CISA National Cyber Exercise Program (NCEP)**<br>CEP@HQ.DHS.GOV |

# General Information

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

**Players** have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
**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.
**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 will 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 would take upon receiving the CISA DDoS Advisory or Alert and examines your agency's baseline planning efforts to protect against, detect and respond to a DDoS attack.
    - **Module 2:** This module explores how your organization would handle indicators of a DDoS attack, confirmation of an attack, mitigation, and monitoring and recovery efforts.
    - **Module 3:** This optional module explores an additional subversive threat discovered during the monitoring and recovery phase, leveraging other existing CISA Tabletop Exercise Packages (CTEPs) materials.
- 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 will be held in an open, no-fault environment. Varying viewpoints are expected.
- Respond to the scenario using your knowledge of existing plans and capabilities, and 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 and possible solutions and/or 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.
- The scenario has been developed in collaboration with subject matter experts and exercise planners from your organization.
- In any exercise, assumptions and artificialities are necessary to complete play in the time allotted, to achieve training objectives, and/or account for logistical limitations. Please do not allow these considerations 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 FCEB DDoS Preparedness

CISA releases a FCEB Advisory describing increased DDoS activity targeting both U.S. and foreign government entities. Recent online activity by known cyber threat actors indicate additional planned attacks targeting U.S. infrastructure including airports, marine terminals, logistics facilities, weather monitoring centers, healthcare, metro systems, exchanges, and trading platforms. This document serves as an advisory to FCEB agencies with associated recommendations for DDoS detection, response, and mitigation strategies.

### *Discussion Questions*

Discussion questions included in each module may be modified as desired. Additional questions can be found in Appendix A.

1. Within your agency, who receives the FCEB DDoS Advisory?
2. Who would your agency share the Advisory with, both internally and externally?
3. What action would your agency take in response to the Advisory?

## Day 3 Agency Review of DDoS Preparedness

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*

4. How would your agency identify all services exposed to the public internet and the vulnerabilities to each of those services?
5. 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)?
    a. What additional protection against DDoS attacks might your agency consider?
    b. What gaps or limitations in coverage exist?
6. 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?
7. What automated and manual methods of DDoS attack detection has your agency implemented?
    a. Who in your agency is notified by the automated detection tools?
    b. How would your agency manually detect a DDoS attack?
    c. How would your agency confirm the DDoS attack?
8. What is the process to ensure all incidents/major events are included in required annual Federal Information Security Modernization Act (FISMA) reporting?

9. Has your agency incorporated DDoS attack response into response plans/your agency CIRP?
    a. How does your agency respond to and rapidly recover from DDoS attacks?
    b. How does your agency identify the type of DDoS attack? Is it documented in your plan?
    c. How are key personnel trained on roles and responsibilities during a DDoS attack?
10. How does your agency notify upstream service providers you are experiencing a DDoS attack?
11. What automated and manual DDoS attack mitigation systems/techniques are available to your agency?
12. How does your agency test their automated and manual DDoS attack mitigation systems/techniques and what is the frequency of testing?
    a. What gaps, best practices or lessons learned have you captured from the tests?
13. How does your agency continue monitoring and mitigating other cyber-attack vectors during a DDoS attack?
    a. What technical and personnel resources are available to continue monitoring and mitigating against other attack vectors?
14. Has your agency exercised its CIRP against a DDoS attack?
    a. What lessons learned (LL) or areas for improvement (AFI) have you identified?
    b. If LL or AFIs were identified, were actions taken to correct or improve the CIRP?

# Module 2

Almost three weeks have passed since the CISA Advisory was released. Today is the day before a federal holiday. Many agency employees are on leave.

## Day 20: Indicators of a DDoS Attack

The agency IT helpdesk experiences a significant increase in the number of teleworking employees reporting they are unable to remotely access the agency network.

The primary public-facing website for your agency that receives significant daily traffic is unavailable. Users on social media platforms are complaining of being unable to access your agency's site.

Your agency's customer service center receives calls from customers and/or stakeholders who cannot access their accounts via the agency website. They report receiving a "page not found" message when attempting to login.

Your outsourced <ISP, MSP, CSP (select one or more)> provider reports issues with your agency's website(s).

### *Discussion Questions*

1. How would the reduced staffing around the holiday impact agency response efforts? How would you overcome any staffing deficiencies?
2. What happens when the IT helpdesk receives an increase in similar calls?
    a. How does the helpdesk know there may be a bigger issue?
    b. What are the processes for notifying and/or escalating this issue?
3. What happens when the public facing customer service call center receives an influx of similar calls?
    a. How does the customer service call center know there may be a bigger issue?
    b. What are the processes for notifying and/or escalating this issue?
4. How does your agency aggregate network disruptions from the IT helpdesk and customer service call center?
5. How does your agency monitor social media for trending activity relevant to your agency?

## Day 20: Confirmation of Attack

Network monitoring tools indicate irregular patterns of incoming traffic.

News organizations have contacted your agency to inquire about the inaccessibility of public-facing websites.

### *Discussion Questions*

6. How would your agency confirm it is experiencing a DDoS attack?
7. What steps would your agency take once the DDoS attack is confirmed?

8. What measures can you immediately put in place to reduce the impact?
    a. What additional actions might be included in your CIRP/Response Playbook/response plan(s)?
    b. Who would implement these actions?
9. How will cascading effects of the DDoS be mitigated?
10. Who would you notify internally and externally?
    a. Describe the federal notification requirements and process upon confirmation of the incident.
11. How would <your agency> respond to the media reports?
    a. Does <your agency> have pre-drafted statements in place to respond to media outlets?
12. What information are you sharing with personnel agency-wide?
    a. How are agency personnel trained to respond to media inquiries?

## Day 20: Understanding the Type of DDoS Attack

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.

### *Discussion Questions*

13. How would your agency determine the type of DDoS attack? Is the technique different depending on the layer it is affecting?
14. Does the incident severity level or tier of this incident change once the type of DDoS attack is determined?
15. How would your agency's mitigation approach change upon understanding the type of DDoS attack?
    a. What are the specific actions your agency would take?
    b. How are roles and responsibilities for mitigation actions defined and assigned?

## Day 20: Mitigation

Mitigation tactics were successful. Teleworkers can access internal networks. Websites are functioning normally.

### *Discussion Questions*

16. How will your agency collect and preserve incident data?
    a. How do you capture and share relevant log data and threat indicators?
    b. What type of digital forensics collection capabilities does your agency have in place?
    c. Are the capabilities internal to your agency or do you rely on another agency or

third-party vendor?

i. If your agency relies on another agency, is there a Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) in place?

ii. If your agency relies on a third-party vendor, are contracts and activation processes in place? Are they tested?

17. During response efforts, who is monitoring other essential systems to ensure an alternate attack is not taking place?
    a. Describe agency contingency plans to address surge staffing requirements.
18. How is incident recovery status communicated to internal and external partners and/or stakeholders?

## Day 20: Monitoring and Recovery

A <hacktivist, APT or criminal> group claims responsibility for the DDoS attack against the agency via social media.

### *Discussion Questions*

19. How would the agency conduct monitoring for indicators of compromise or nefarious traffic?
20. What additional reports, notifications, and/or coordination are necessary?
21. How and when will your agency transition to the recovery and post-incident phases?
    a. How is the decision to transition to the recovery phase made?
    b. How does your agency conduct post-incident review?
    c. How are LL/AFIs incorporated into the agency's Continuous Improvement Planning (e.g., incident response plans, training, etc.)?
22. What measures can your agency put in place to prevent and mitigate future DDoS attacks?

## Module 3 (Optional)

Module 3 is the optional exploration of an additional subversive threat discovered during the monitoring and recovery phase. The CISA CTEP library contains threat scenarios to extend this TTX, including:

- Insider Threat
- Ransomware
    - Ransomware Third Party Vendor
- Vendor Phishing

# Appendix A: Additional Discussion Questions

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

## Reporting and Notifications

1. Describe <your agency's> reporting and notification requirements
    a. How does <your agency> differentiate between an incident and a major incident?
    b. How does the notification requirement for <your agency> differ between the two?
    c. What timeframes are involved for reports/notifications?
    d. What information must be included in the reports/notifications?
    e. What additional reporting is required for <your agency>, other than CISA and the Office of Management and Budget (OMB)?

## Public Affairs

1. What information would <your agency> communicate to the public? How would you communicate it?
    a. How would <your agency> respond to the complaints on social media? Would you use social media or respond by drafting statements?
    b. Does <your agency> have pre-drafted statements in place to respond to complaints on social media?
2. Are public affairs personnel trained to manage messaging related to cyber incidents?
3. How would <your agency> respond to any attempts at disinformation/misinformation by the group responsible for the DDoS attack or any other malicious actors?

# Appendix B: Acronyms

| Acronym | Definition |
|---|---|
| AAR | After-Action Report |
| AFI | Areas for Improvement |
| APT | Advanced Persistent Threat |
| CIRP | Cybersecurity Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CSP | Cloud Service Provider |
| CTEP | CISA Tabletop Exercise Packages |
| DDoS | Distributed Denial of Service |
| FCEB | Federal Civilian Executive Branch |
| FISMA | Federal Information Security Modernization Act |
| IS | Information Systems |
| ISP | Internet Service Provider |
| IT | Information Technology |
| LL | Lessons Learned |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| MSP | Managed Service Provider |
| NCEP | National Cyber Exercise Program |
| 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 Distributed Denial of Service Attacks on U.S. Infrastructure and Government Websites*

Summary: 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.

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 used existing measures to address the attack, minimizing down time. The network was not compromised, and no data was lost as a result of the attack.[1]

Wednesday, October 5, 2022

Public facing state websites in Colorado, Kentucky and Mississippi were disrupted by a large-scale DDoS attack. Some of the sites were restored by that afternoon. Colorado's website was restored the next day. According to spokespersons for the states, while the public facing websites were unavailable, critical services were on-line and available.[2]

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.[3]

The DDoS attack did not impact flights.

## *New Zealand Institutions Suffer Repeated Targeted DDoS Attacks*

September 2021

Multiple New Zealand government and commercial organizations such as banks, the postal service, the weather service, and news organizations were victims of a coordinated DDoS attack following a major attack against the nation's third-largest ISP.

In 2020, multiple New Zealand organizations were also hit by DDoS attacks after receiving extortion notices shortly before the attacks began. New Zealand's stock exchange (NZX) public website was

---

[1] Vicens, A.J. (2022, July 8). Pro-Russian cybercriminals briefly DDoS Congress.gov. *CyberScoop*. https://www.cyberscoop.com/killnet-congress-ddos-russia-hacktivist/

[2] Lyngaas, S. (2022, October 8). Russian-speaking hackers knock US State government websites offline. *CNN*. https://www.cnn.com/2022/10/05/politics/russian-hackers-state-government-websites/index.html

[3] Toulas, B. (2022, October 10). US airports' sites taken down in DDoS attacks by pro-Russian hackers. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers/

down for five days, significantly disrupting operations.[4] Other organizations suffered days-long outages. [5] The attacks on NZX pushed over a terabit of spurious data per second.[6]

[4] Menon, P. (2020, August 30). New Zealand bourse website hit by fresh cyberattack, but keeps trading. *Reuters.* https://www.reuters.com/article/us-nzx-cyber/new-zealand-bourse-website-hit-by-fresh-cyberattack-but-keeps-trading-idUSKBN25R004

[5] Whelan, M. (2022, September 8). DDoS attacks: What they are and how they're orchestrated. *Radio New Zealand*. https://www.rnz.co.nz/news/national/451063/ddos-attacks-what-they-are-and-how-they-re-orchestrated.

[6] Pullar-Strecker, Tom. (2020, September 2). GCSB examining extortion email sent to NZX ahead of DDoS attack. *Stuff.* https://www.stuff.co.nz/business/122636582/gcsb-examining-extortion-email-sent-to-nzx-ahead-of-ddos-attack

# Appendix D: Attacks and Facts

## 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
- CISA DDoS Quick Guide
  https://www.cisa.gov/uscert/security-publications/DDoS-Quick-Guide
- CISA Alert: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure:
  https://www.cisa.gov/uscert/ncas/alerts/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
- CISA Understanding Denial-of-Service Attacks
  https://www.cisa.gov/uscert/ncas/tips/ST04-015
- UK National Cyber Security Center DoS Guidance
  https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

# Appendix E: Additional Resources

## Principal Doctrine

- Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013)
  http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- Framework for Improving Critical Infrastructure Cybersecurity (2018)
  https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- National Infrastructure Protection Plan (NIPP) 2013
  http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience
- National Institute of Standards and Technology Computer Security Incident Handling Guide Rev 2 (2012)
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- National Response Framework (2019)
  https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf
- Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017)
  https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2013)
  https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- Presidential Policy Directive 41: United States Cyber Incident Command (2016)
  https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
- Annex to Presidential Policy Directive 41: Annex to the Directive on United States Cyber Incident Coordination (2016)
  https://www.hsdl.org/?view&did=797545
- National Cyber Incident Response Plan (NCIRP) (2016)
  https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
- CISA National Cyber Incident Scoring System (NCISS)
  https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
  Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) | CISA

## Key Points of Contact

- CISA Integrated Operations Center (contact: central@cisa.dhs.gov)
- United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact: http://www.secretservice.gov/contact/field-offices)
- Federal Bureau of Investigation (FBI) Field Office Cyber Task Forces http://www.fbi.gov/contact-us/field
- FBI Internet Crime Complaint Center (IC3) http://www.ic3.gov
- National Cyber Investigative Joint Task Force (NCIJTF) 24/7 Command Center (contact: cywatch@ic.fbi.gov; 855-292-3937)

## References Cited

Lyngaas, S. (2022, October 8). Russian-speaking hackers knock US State government websites offline. *CNN*. https://www.cnn.com/2022/10/05/politics/russian-hackers-state-government-websites/index.html

Menon, P. (2020, August 30). New Zealand bourse website hit by fresh cyberattack, but keeps trading. *Reuters.* https://www.reuters.com/article/us-nzx-cyber/new-zealand-bourse-website-hit-by-fresh-cyberattack-but-keeps-trading-idUSKBN25R004

Pullar-Strecker, Tom. (2020, September 2). GCSB examining extortion email sent to NZX ahead of DDoS attack. *Stuff.* https://www.stuff.co.nz/business/122636582/gcsb-examining-extortion-email-sent-to-nzx-ahead-of-ddos-attack

Toulas, B. (2022, October 10). US airports' sites taken down in DDoS attacks by pro-Russian hackers. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers/

Vicens, A.J. (2022, July 8). Pro-Russian cybercriminals briefly DDoS Congress.gov. *CyberScoop*. https://www.cyberscoop.com/killnet-congress-ddos-russia-hacktivist/

Whelan, M. (2022, September 8). DDoS attacks: What they are and how they're orchestrated. *Radio New Zealand*. https://www.rnz.co.nz/news/national/451063/ddos-attacks-what-they-are-and-how-they-re-orchestrated