CAPACITY ENHANCEMENT GUIDE
Additional DDoS Guidance for Federal Agencies

October 28, 2022

PURPOSE

In October 2022 the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released Understanding and Responding to Distributed Denial-of-Service Attacks, which encourages organizations to take proactive steps to reduce the likelihood and impact of DDoS attacks. This Capacity Enhancement Guide provides federal civilian executive branch (FCEB) agencies additional DDoS guidance that includes recommendations of contract vehicles and services specifically designed for, and only available to, FCEB agencies.

AT-A-GLANCE RECOMMENDATIONS

- Review joint Understanding and Responding to Distributed Denial-of-Service Attacks.
- Consider using GSA Enterprise Infrastructure Solutions vehicles:
  - Managed Security Service (MSS)
  - Managed Trusted Internet Protocol Service (MTIPS)
- Consider using GSA Highly Adaptive Cybersecurity Services

AUDIENCE & SCOPE

This guide:

- Recommends additional capabilities to protect FCEB networks against DDoS attacks.
- Provides information to inform FCEB agency executive leadership.
- This guide is not intended for or applicable to state, local, tribal, and territorial governments, and commercial industry.
- Supports CISA's role as the nation's cybersecurity risk advisor by sharing high-priority recommendations, best practices, and operational insights in response to systemic threats, vulnerabilities, and risks.

RECOMMENDATIONS

In addition to the recommendations provided by Understanding and Responding to Distributed Denial-of-Service Attacks, FCEB agencies should:

- Ensure to include all identified High Value Assets (HVAs) when assessing critical assets and services for vulnerabilities and exposure to the internet.
- Enroll all publicly exposed assets in CISA's Cyber Hygiene Services and verify appropriate configurations of the existing monitoring tools.
- Conduct at least one agency-level DDoS tabletop exercise. CISA encourages agencies to use the CISA DDoS Tabletop Exercise Package.

As mentioned in Understanding and Responding to Distributed Denial-Of-Service Attacks, many ISPs have DDoS protections, but a dedicated DDoS protection service would likely provide more robust protections against larger or more advanced DDoS attacks. Agencies should evaluate current defenses against DDoS, verify DDoS protections are in place, and consider implementing more robust protections if the agency determines its current protections may be lacking. Agencies without comprehensive DDoS protection may take advantage of the following options:

- Enterprise Infrastructure Solutions (EIS) – a comprehensive, solution-based contract vehicle to address all federal agency IT telecommunications and infrastructure requirements. Under EIS, federal agencies have access to:
  - Managed Security Service (MSS) – a comprehensive service that protects an agency's IT assets from malicious attacks. The Incident Response Service (INRS) under MSS provides an effective method of combatting and documenting security intrusions. INRS processes can detect a DDoS attack and provide processes and security tools to counter the DDoS attack and restore operation of the system.
  - Managed Trusted Internet Protocol Service (MTIPS) – an orderable solution for the CISA Trusted Internet Connections (TIC) 3.0 Traditional Use Case modeled after the perimeter-based internet security paradigm. TIC services offer protections against DDoS attacks. Agencies utilizing TIC services should consult with their solution providers and consider subscribing to additional DDoS protection and mitigation services under MTIPS if necessary.

  CISA encourages agencies to reach out to their GSA Solutions Broker (SB) for assistance with reviews of their current architecture to identify areas for modernization and for support leveraging GSA tools, products, and services. GSA SB contact information by agency can be found at GSA's Telecommunications Services Customer Support website.
- Highly Adaptive Cybersecurity Services (HACS) - the HACS contract vehicle gives agencies ready access to pre-vetted cybersecurity services, including HVA assessments, risk and vulnerability assessments, cyber hunt, incident response, and penetration testing. HACS HVA assessments offer security architecture review (SAR) capabilities, which evaluate and inform management of properly architected cyber solutions. These services allow agencies to better understand their current risk posture and explore ways to implement a recommended securely architected cyber solution. HVA assessments also perform systems security engineering (SSE) services, which help identify vulnerabilities in common security areas (e.g., perimeter security, network security, endpoint security, and application security). HACS assist with preparing for and guarding against cyber threats, including DDoS attacks.

REPORTING

Agencies should follow all relevant CISA protocols and OMB guidance when reporting events, incidents, breaches, and major incidents. This includes CISA's current Federal Incident Notification Guidelines, CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks, OMB M-22-05 and OMB M-17-12, and Presidential Policy Directive 41 (PPD-41).

CONTACT INFO

For questions about this guidance and other CISA services available to federal agencies, please contact cyberliaison@cisa.dhs.gov.

RESOURCES

CISA/FBI/MS-ISAC Guide: Understanding and Responding to Distributed Denial-of-Service Attacks

GSA: Enterprise Infrastructure Solutions Resources

GSA: Trusted Internet Connections (TIC)

GSA: Highly Adaptive Cybersecurity Services (HACS)

GSA: Telecommunications Services Customer Support

CISA: Tabletop Exercise Packages

Last updated: October 28, 2022