Coalition for Cybersecurity
Policy and Law

Coalition for Cybersecurity Policy and Law
575 Seventh Street, NW, Washington, DC 20004

July 27, 2017

VIA EMAIL: counter_botnet_RFC@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Attn: Evelyn L. Remaley, Deputy Associate Administrator
Washington, DC 20230

Re: Comments of the Coalition for Cybersecurity Policy & Law

The Coalition for Cybersecurity Policy & Law ("Coalition") submits this comment in response to the Request for Comments ("RFC") issued by the National Telecommunications and Information Administration ("NTIA") on June 13, 2017.[1] The NTIA's RFC sought input on current and potential approaches for dealing with botnets and similar threats. In particular, the RFC solicited comments on mitigating the impact of botnet attacks and securing devices to prevent the spread of botnet malware.[2] The Coalition appreciates the opportunity to provide these comments and participate in this important discussion. The Coalition believes that finding a solution to the issues identified in the NTIA's RFC requires close cooperation amongst private companies and government agencies both within the United States and internationally. The Coalition further believes that the Department of Commerce ("the Department") can play a key role in this effort by bringing these entities together and facilitating the development of voluntary, consensus-based, industry-led standards relating to responding to botnet attacks and securing devices against botnet malware.

The Coalition is comprised of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[3] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management, and we are supportive of efforts to identify and promote the adoption of cybersecurity best practices and voluntary standards throughout the global community.

Botnets present a serious and growing threat to the online economy. They are frequently used to distribute malware, including ransomware, and to launch Distributed Denial of Service

[1] 82 Fed. Reg. 27042 (June 13, 2017) (Docket No. 170602536-7536-01).
[2] *Id.* at 27043.
[3] The views expressed in this comment reflect the consensus views of the Coalition, and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, see www.cybersecuritycoalition.org.

("DDoS") attacks.[4] These attacks can be very costly for businesses, and are occurring with greater frequency and at an unprecedented scale. In just the last year, the frequency of DDoS attacks against companies that experience more than 10 attacks per month has increased by 38%.[5] The scale of these attacks has also increased significantly with DDoS attacks now exceeding one terabit per second.[6]

The increasing frequency and scale of attacks launched using botnets can be explained, in part, by the increasing number of devices that are controlled by botnets and the growth of the Internet of Things ("IoT"). Despite efforts to take botnets offline, the number of bots increased between 2015 and 2016 from 91.9 million to 98.6 million.[7] Botnet operators have also increasingly targeted IoT devices. In the last year, IoT devices were attacked at twice the frequency of the year prior, and the first botnet using IoT devices was involved in the largest DDoS attack ever recorded.[8] The number of IoT devices in the United States is also predicted to nearly double between 2015 and 2020, increasing from 2.3 billion devices to 4.1 billion.[9] Globally, the number of IoT devices is expected to increase from 16 billion to 26 billion in the same period.[10] We are experiencing unprecedented growth in the number and nature of devices being added to the global Internet, including a wide array of low cost IoT devices. Unless more work is done to increase the baseline security of such devices and the intelligence of the network, we expect to see continued growth in the frequency and scale of distributed attacks that threaten the functionality of critical systems and the availability of essential information. Although the threat presented by botnets is clear, their adaptive and distributed nature make identifying botnets and taking them offline difficult. At the same time, botnet operators have been able to exploit social engineering techniques and inherent challenges in securing IoT devices to continue to grow the size of their botnets.[11] The Coalition believes that the challenges presented by botnets should be addressed through a combination of the development of voluntary, consensus-based, industry-led standards and coordination amongst private and public entities both within the United States and internationally.

The Coalition believes that the Department can play an important role in facilitating the development of industry best practices and bringing together the many parties that are needed to take down botnets and prevent the spread of botnet malware. Specifically, the Coalition encourages the Department to: (1) facilitate the development and adoption of industry best practices for both device and network security; (2) promote the sharing of cyber threat indicators; and (3) promote efforts to educate users on the threat presented by botnet malware and how to

[4] Symantec, *Internet Security Threat Report*, 8, 24 (April 2017) ("Symantec").

[5] Arbor Networks, *Worldwide Infrastructure Security Report*, 75 (2017).

[6] Cisco Systems, 2017 Midyear Security Report, 39 (July 2017). *See also*: "150,000 IoT Devices Abused for Massive DDoS Attacks on OVH," by Eduard Kovacs, *SecurityWeek*, September 27, 2016: securityweek.com/150000-iot-devices-abused-massive-ddos-attacks-ovh.

[7] Symantec at 41.

[8] *Id.* at 8.

[9] The Department of Commerce, Fostering the Advancement of the Internet of Things, 4 (January 2017)(citing Cisco, VNI Complete Forecast Highlights Tool (2016), http://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html).

[10] *Id.*

[11] Symantec at 59.

identify attacks on their devices. The Coalition recognizes that NTIA has already begun work in some of these areas and encourages the NTIA to continue this critically important work.

I. The Department Should Facilitate the Development and Adoption of Industry Best Practices to Secure Users' Devices

The Coalition applauds the Department's efforts to facilitate the development of best practices in the areas of vulnerability reporting and IoT security upgradability and patching and encourages the Department to continue these efforts.[12] The Coalition further encourages the Department to initiate multistakeholder processes to develop industry standards promoting secure product development practices and strong network security measures to better protect IoT devices against botnet malware. The Department should also promote broad adoption of the NIST Cybersecurity Framework with a particular focus on adoption by IoT device manufacturers.

Product Development. The Coalition believes that there is a particular need for consensus-based, voluntary standards with respect to the development of secure IoT devices. While securing some types of IoT devices is challenging due to the low cost of the device, low power consumption requirements, and other factors,[13] the development of voluntary standards that account for the wide variety of devices and security needs in the IoT market is likely to help IoT device manufacturers implement better security measures where possible. Improving the security of IoT devices will help diminish the impact of botnet attacks by making it more difficult for botnet operators to add new devices to their botnets. For example, the Mirai botnet searches for IoT devices that use well-known default passwords.[14] Therefore, to protect against the Mirai botnet and other malware, IoT device manufacturers should not ship their devices using default password settings or should require consumers to change the password as part of the installation process. IoT device manufacturers should also ensure that they are performing appropriate security testing of their software to identify vulnerabilities before making their products available to consumers. The Coalition also believes it is vital that secure software development and patching be considered. This includes providing training to the relevant personnel on secure coding and product development practices, implementing appropriate procedures to minimize the inclusion of known vulnerabilities in code development, and regularly updating and patching device software using secure transmission pathways for these updates. We also believe that effective management of risk from IoT devices will increasingly require intelligent interactions between those devices and the networks in which they operate.[15]

[12] *See* NTIA, *Multistakeholder Process: Cybersecurity Vulnerabilities*, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities; NTIA, *Multistakeholder Process: Internet of Things (IoT) Security Upgradability and Patching*, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

[13] Cisco, *Securing the Internet of Things: A Proposed Framework*, available at http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html.

[14] McAfee Labs, *Threats Report*, 17 (April 2017).

[15] For example, the voluntary consensus-based standards may help promote more robust security interactions between devices and the networks that manage them. *See*: https://tools.ietf.org/html/draft-ietf-opsawg-mud-02 (proposed standard to enable detection of anomalous device behavior as compared to manufacturer specifications) and https://tools.ietf.org/html/draft-ietf-anima-bootstrapping-keyinfra-05 (proposed standard for zero-touch secure provisioning of devices into established network domains).

Adoption of the NIST Framework. The Coalition believes that broader adoption of the Framework, particularly by IoT device manufacturers, Web hosting companies, ISPs, and enterprises will result in better security, which in turn will make it more difficult for botnet operators to succeed. The Framework provides companies with a flexible, adaptive, and voluntary construct that enables them to make risk-informed decisions regarding security and to measure their progress towards their security goals. Because the Framework is adaptable, it can be used by companies of all sizes to improve security outcomes, making it particularly well-suited for the IoT market, which includes a wide variety of products with different technical capabilities and security needs.

The Coalition also believes there is utility in developing specific applications of the Framework to address particular security issues. Accordingly, the Coalition has created a DDoS threat profile under the Cybersecurity Framework (attached). We believe that this profile could be a starting point to help NTIA and NIST promote adoption of the Framework in ways that will minimize the impact of DDoS including in the organizations mentioned above and in Federal government agencies.

II. The Department Should Promote the Sharing of Cyber Threat Indicators and Facilitate the Development of International Standards for Sharing Cyber Threat Indicators

The Coalition encourages the Department to facilitate the development of voluntary, consensus-based standards that will encourage organizations to implement automated information sharing mechanisms to promote the sharing of cyber threat indicators relating to botnets amongst industry participants and with the appropriate government agencies.[16] Sharing threat indicators, enables organizations to proactively implement security measures. Sharing threat indicators should help prevent botnet operators from gaining control of devices and other network-based resources and enable organizations to more easily identify previously infected devices. Such information sharing will also help other organizations secure the devices on their networks, which limits the number of devices that a botnet can infect

Sharing cyber threat indicators with the appropriate government agencies may also help with the identification of a botnet and facilitate taking botnets offline. Cooperation between industry participants and law enforcement is critical to identifying the command and control servers for a botnet and dismantling the network. The Department should facilitate discussions between industry participants and law enforcement to identify how such sharing of cyber threat

[16] Given the continued proliferation of endpoint devices and the related increasing number and size of botnets, it is vital that cyber threat information sharing mechanisms are capable of automation. This will free humans to focus on the problems that require more sustained attention and creativity. Such automated mechanisms should leverage existing standards and specifications for threat sharing, such as the Trusted Automated eXchange of Indicator Information (TAXII); the Structured Threat Information eXpression (STIX); and the Cyber Observable eXpression (CybOX).

indicators can take place more efficiently and how to encourage more industry participants to share cyber threat indicators with law enforcement.[17]

The global nature of botnets necessitates that industry participants and law enforcement agencies across a number of countries cooperate to identify and take botnets offline. The Department can play an important role in facilitating this cooperation by promoting the development of international standards for sharing cyber threat indicators. The creation of common standards for the sharing of cyber threat information will enable companies to take a more proactive approach to defending their networks against botnets. It may also have a deterrent effect on botnet operators by increasing the cost of adding devices to the botnet. It may further enable law enforcement to more efficiently investigate botnets and take them down.

III. The Department Should Encourage Industry Efforts to Inform Consumers and Employees about Measures They Can Take to Protect their Devices

With many botnets delivering malware as an attachment to an email, the Coalition believes that companies should coordinate to educate consumers on how to identify emails that may contain malware and what to do if they suspect that their device may be infected. The Department can promote these efforts by facilitating a discussion amongst industry participants about effective means to provide this information to consumers. The Department should also promote current industry efforts to educate consumers regarding good security practices. A number of the Coalition's members participate in the "Stop. Think. Connect." campaign, which provides consumers with information about protecting the security of their information and devices while online.[18] While consumer education is not a complete answer to the problem, cooperative education efforts like the "Stop. Think. Connect" campaign can provide consumers with the knowledge they need to recognize a suspicious email and avoid downloading malware by clicking on an attachment.

In addition to informing consumers how to protect themselves online, the Coalition believes that contextual customer notification may enable consumers to respond in the event their device is infected by malware. Notifying consumers that their devices are infected by malware may not help consumers if they do not have the tools to remove the malware or are not able to distinguish between authentic notifications and fraudulent ones. Alternatively, where a company refers a consumer to a tool that enables the consumer to identify the problem and take remedial action, such notice can effectively reduce the number of devices that are part of a botnet. The Department should facilitate this effort to provide consumers with contextual notice by bringing industry participants together to develop guidance for companies that choose to provide such notice to their customers.

The Department should also encourage companies to provide appropriate education and training to their employees regarding the secure use of any devices that the company provides to

[17] The Department should work together with the Department of Homeland Security and the Department of Justice to evaluate the effectiveness of existing programs, such as Automated Indicator Sharing (AIS), and to ascertain whether they can be used to manage the risk of DDoS attacks that leverage IoT devices and/or botnets.
[18] The Stop. Think. Connect. website is available at https://www.stopthinkconnect.org.

its employees. This training should provide employees with information about identifying malicious emails containing malware and how to avoid otherwise downloading malware.

V. Conclusion

The Coalition thanks the NTIA for the opportunity to comment in this important effort. We look forward to working with you as this process moves forward and to participating in any further discussions regarding measures that can be implemented to address threat presented by botnets.

Sincerely,

Ari Schwartz
Coordinator

Cybersecurity Framework DDoS Profile

Executive Summary

The Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) version 1.0, developed by the National Institute of Standards and Technology (NIST), with extensive private sector input, provides a risk-based and flexible approach to managing cybersecurity risk that incorporates industry standards and best practices. The Cybersecurity Framework is by design crafted to allow individual organizations to determine their own unique risks, tolerances, threats and vulnerabilities, so that they may prioritize their resources to maximize effectiveness.

The Framework is general in nature to allow for broad applicability to a variety of industries, organizations, risk tolerances and regulatory environments. A Framework Profile is the application of Framework components to a specific situation. A Profile may be customized to suit specific implementation scenarios by applying the Framework Category and Sub-Categories appropriate to the situation. Profiles should be constructed to take into account the organization's:

- Business/mission objectives
- Regulatory requirements
- Operating environment

Organizations can use Profiles to define a desired state for their Cybersecurity posture based on their business objectives, and use it to measure progress towards achieving this state. It provides organizations with the ability to analyze cost, effort and risk for a particular objective. Profiles may also be used by industry sectors to document best practices for protection against specific threats.

The below Cybersecurity Framework Profile focuses on Distributed Denial of Service (DDoS). DDoS attacks are increasing in complexity, size, and frequency, and the range of targets and methods (e.g., from using individual PCs to using connected Internet of Things (IoT) devices) has also broadened. This threat profile emphasizes how the Cybersecurity Framework can address DDoS attacks, which NIST has acknowledged is a growing risk.

To develop the threat profile, we have reviewed all the Cybersecurity Framework Categories and Subcategories and determined those most important to combat the DDoS threat. The Categories and Sub-Categories were then labeled into different priorities as follows:

P1 – Minimum actions required to protect network and services against DDoS attacks

P2 – Highly recommended actions to protect network and services against DDoS attacks

P3 – Recommended actions to protect network and services against DDoS attacks.

The DDoS threat mitigation profile represents a Target Profile focused on the desired state of organizational cybersecurity to mitigate DDoS attacks. It may be used to assist in identifying opportunities for improving DDoS threat mitigation and aiding in cybersecurity prioritization by comparing current state with this desired Target state.

In the development of this profile we did not identify the need for any additions or changes at the Category or Subcategory level. Instead, the comments provided as part of the profile give the necessary guidance to refine the understanding of the Subcategory as it applies to DDoS threat mitigation.

Overview of the DDoS Threat

A DDoS attack attempts to overwhelm a network, service or application with traffic from multiple sources. There are many methods for carrying out DDoS attacks. These can include

- Low bandwidth connection oriented attacks designed to initiate and keep many connections open on the victim exhausting its available resources.
- High bandwidth volumetric attacks that exhaust available network or resource bandwidth.
- Protocol oriented attacks that take advantages of stateful network protocols such as TCP.
- Application layer attacks designed to overwhelm some aspect of an application or service.

Although each of these methods can be highly effective, in recent years, there has been considerable attention given to volumetric attacks as the result of several high-profile incidents.

One prominent example of a volumetric DDoS attack vector is reflection amplification. This is a type of DDoS attack in which the attacker fakes the attack target’s IP address and launches queries from this address to open services on the Internet to solicit a response. The services used in this methodology are typically selected such that the size of the response to the initial query is many times (x100s) larger than the query itself. The response is returned to the real owner of the faked IP. This attack vector allows attackers to generate huge volumes of attack traffic, while making it difficult for the target to determine the original sources of the attack traffic. Reflection amplification has been responsible for some of the largest DDoS attacks seen on the Internet through the last decade.

Attackers can build out their attack capability in many ways, such as the use of malware to infect Internet connected computers, deploying servers within hosting environments, exploiting program flaws or other vulnerabilities, and by exploiting the use of inadequate access controls on Internet connected devices to create botnets.

Botnets are created when an attacker infects or acquires a network of hosts, then controls these devices to remotely launch an attack at a given target. Increasingly, botnets are incorporating Internet of Things (IoT) devices, which continue to proliferate at a remarkable rate. Botnets allow for a wide variety of attack methods aimed at evading or overwhelming defenses.

DDoS is often referred to as a 'weaponized' threat as technical skills are no longer needed to launch an attack and services to conduct DDoS have proliferated and become easily obtainable for relatively low cost.

Availability is a core information security pillar but the operational responsibility and discipline for assessing and mitigating availability-based threats such as DDoS often falls to network operations or application owners in addition to Risk and Information Security teams. Because of this divided responsibility, fissures in both risk assessment and operational procedures for addressing these threats may occur. The goal of this profile is to ensure the strategic and operational discipline needed to protect and respond to DDoS threats is comprehensively addressed by applying the appropriate recommendations and best practices outlined in the Cybersecurity Framework.

DDoS Threat Mitigation Profile

Function	*Category*	*Sub-Category*	*Priority*	*Framework Comment*
Identify (ID)	**Asset Management (ID.AM)**	**ID.AM-1:** Inventory physical devices and systems within the organization	**P2**	Catalog critical Internet facing services by location and capacity Catalog ISP connectivity by ISP, bandwidth usage, bandwidth available
		ID.AM-2: Inventory software platforms and applications within the organization	**P1**	Determine critical Internet facing services by type of application/service, IP address and hostname

Function	Category	Sub-Category	Priority	Framework Comment
		ID.AM-3: Map organizational communication and data flows	**P2**	Identify key stakeholders in the organization critical to availability of Internet facing services including application owners, security personnel, network operations personnel, executive leadership, legal/risk personnel and ISP or Cloud based DDoS mitigation service providers Maintain network maps showing data flows Create an operational process document detailing communication workflows
		ID.AM-4: Catalogue external information systems	**P3**	Identify applications and services that are run in cloud, SaaS, hosting or other external environments
		ID.AM-5: Resources are prioritized based on their classification, criticality, and business value	**P2**	Determine what Internet facing services will result in the most business impact if they were to become unavailable
	Business Environment (IDE.BE)	**ID.BE-4:** Establish dependencies and critical functions for delivery of critical services	**P2**	Catalog external dependencies for services and applications including DNS, NTP, cloud/hosting provider, partner network connections and Internet availability
		ID.BE-5: Establish resilience requirements to support delivery of critical services	**P3**	Ensure geographical redundancy and high availability of equipment providing services, network infrastructure and Internet connections

Function	Category	Sub-Category	Priority	Framework Comment
	Risk Assessment (ID.RA)	**ID.RA-1:** Identify and document asset vulnerabilities	P2	Determine network and application bottlenecks including throughput, connection rate and total connections supported
		ID.RA-2: Cyber threat intelligence and vulnerability information is received from information sharing forums and sources	P3	Monitor vulnerabilities lists (CVE, NVD and similar) to check if critical Internet facing services have vulnerabilities that could be used as a condition for Denial of Service.
		ID.RA-3: Identify and document internal and external threats	P3	Continuously gather industry information around DDoS trends, peak attack sizes, frequency, targeted verticals, motivations and attack characteristics
		ID.RA-4: Identify potential business impacts and likelihoods	P2	Create a risk profile that quantifies potential cost of recovery operations per DDoS incident, revenue loss, customer churn, brand damage and impact to business operations
	Governance (ID.GV)	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	P1	Put processes in place to ensure all regulatory requirements are met. Train all personnel responsible for DDoS incident response on the relevant legal and regulatory requirements surrounding the data that they may handle. Document regulatory and data privacy policies of DDoS service providers and partners

Function	Category	Sub-Category	Priority	Framework Comment
Protect (PR)	**Awareness and Training (PR.AT)**	**PR.AT-2:** Privileged users understand roles & responsibilities	P1	Security Operations personnel have been trained on DDoS defense processes, products and services Equip security operations personnel with an operational run book defining what process to follow and who to contact should an incident take place
	Information Protection Processes and Procedures (PR.IP)	**PR.IP-1:** Create and maintain a baseline configuration of information technology/industrial control systems	P1	Create a baseline DDoS protection architecture consisting of best current practices for the network, network based protection capabilities and non-stateful Intelligent DDoS Mitigation capability Implement anti-spoofing and black/white list filtering at network edge Maintain DDoS protection configuration that provides general protection for all services and always on protection for all business-critical assets
		PR.IP-7: Continuously improve protection processes	P2	Conduct a minimum of 2 annual tests of DDoS protection capabilities Perform after-action reviews following all DDoS incidents and DDoS protection tests adjusting DDoS defenses accordingly

Function	Category	Sub-Category	Priority	Framework Comment
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	P3	The organization’s Business Continuity and Disaster Recovery plans should have components to address the potential effects of a DDoS attack
		PR.IP-10: Response and recovery plans are tested	P3	The DDoS components of the Business Continuity and Disaster Recovery plans should be tested.
		PR.IP-12: A vulnerability management plan is developed and implemented	P3	Vulnerabilities that can be leveraged for DDoS events should be documented and remediated.
	Protective Technologies (PR.PT)	**PR.PT-4:** Protect communications and control networks	P1	Perform filtering of traffic to control plane network and/or control plane traffic policing
Detect (DE)	**Anomalies and Events (DE.AE)**	**DE.AE-1:** Establish and manage a baseline of network operations and expected data flows for users and systems	P1	Continuously measure traffic to hosts, resources or groups of resources to determine expected traffic over time. Determine traffic baselines for IP protocols such as TCP, UDP, ICMP, GRE and critical applications such as HTTP, DNS, NTP, SSDPand SIP
		DE.AE-2: Analyze detected events to understand attack targets and methods	P1	Determine source and destination traffic characteristics when anomalous traffic is

Function	Category	Sub-Category	Priority	Framework Comment
				detected that is indicative of DDoS
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	P2	Aggregate data for detected DDoS events from multiple network sources contributing to the attack.
		DE.AE-4: Impact of events is determined	P2	Total traffic rates for DDoS events can be measured across all contributing network sources Performance and availability of services can be measured before, during and after events
		DE.AE-5: Incident alert thresholds are established	P1	Configure notifications to security monitoring personnel and appropriate stakeholders when traffic exceeds measured or configured thresholds
	Security Continuous Monitoring (DE.CM)	**DE.CM-1:** Monitor network to detect potential cybersecurity events	P1	Continuously measure traffic intoall network ingress points and between transit points on the internal network for traffic anomalies To the extent possible and/or practical from a business perspective, continually measure outbound traffic for detection of traffic anomalies that could represent sources contributing to outbound or cross-bound DDoS attacks.

Function	Category	Sub-Category	Priority	Framework Comment
		DE.CM-8: Vulnerability scans are performed	P1	Scan Internet facing services to identify vulnerabilities that can be exploited for participation in DDoS events.
	Detection Processes (DE.DP)	**DE.DP-3:** Test detection processes	P2	Conduct regular testing of DDoS defense capabilities including occasional unannounced tests performed with no prior warning to assess the DDoS defense strategies and processes Conduct DDoS simulation wargames as part of security staff onboarding and periodically for the security response team
		DE.DP-5: Continuously improve detection processes	P2	Perform after-action review on any defense testing or DDoS events after all operations are successfully restored to identify and improve DDoS detection capabilities Identify and maintain key security metrics around detection, identification and escalation effectiveness.
Respond (RS)	**Response Planning (RS.RP)**	**RS.RP-1:** Execute response plan during or after an event	P1	Follow DDoS response run book during any detected DDoS events
	Communications (RS.CO)	**RS.CO-1:** Ensure personnel know their roles and order of operations when a response is needed	P1	Define personnel responsible for detection, mitigation, coordination and communication during DDoS incidents

Function	Category	Sub-Category	Priority	Framework Comment
		RS.CO-4: Coordinate with stakeholders consistently with response plans	P1	Document operational run book that includes roles, responsibilities and escalation process for all parties responsible for DDoS incident response including internal personnel and external consultants or services
		RS.CO-5: Engage in voluntary information sharing with external stakeholders to achieve broader cybersecurity situational awareness	P3	Share and receive DDoS attack trends with consultants, service companies and/or threat intel companies to keep abreast of attack scale, frequency, motivations and evolving attack vectors
	Analysis (RS.AN)	**RS.AN-1:** Investigate notifications from detection systems	P1	Add DDoS alert notifications to monitoring and response systems including security and network operations management systems.
		RS.AN-2: Understand the impact of the incident	P2	Compare DDoS traffic rates, connection rates and total connections against documented system and network limits Identify actual and potential impact to business services, customers, employees and other stakeholders.
		RS.AN-3: Forensics are performed	P3	Save raw anomaly details in available form (logs, packet captures, flow telemetry data) to investigate parties involved in the incident and, where appropriate, to share incident details

Function	*Category*	*Sub-Category*	*Priority*	*Framework Comment*
				with the operational security community.
	Mitigation (RS.MI)	**RS.MI-2:** Mitigate incidents	P1	Mitigate DDoS attacks using any or all of the following: - Network capabilities such as ACLs, anti-spoofing, remote triggered blackhole and/or flow spec - Using intelligent DDoS mitigation systems on premise - Contracting a DDoS mitigation service Critical resources should be protected by always on mitigation capabilities - Contract or coordinate with upstream bandwidth provider for defense against high-magnitude attacks. Implement a notification system to detect when on premise bandwidth is reaching saturation then alert and/or automate movement of traffic to an upstream DDoS mitigation service Identify and maintain key security metrics around mitigation and escalation effectiveness.

Function	Category	Sub-Category	Priority	Framework Comment
	Improvements (RS.IM)	**RS.IM-1:** Incorporate lessons learned into response plans	P2	Adjust mitigation processes, capacity, technology and partnerships based on DDoS attack trends, DDoS response testing and results of DDoS after-action reviews Maintain key security metrics around the DDoS program to demonstrate program improvement and effectiveness.
Recover (RC)	**Recovery Planning (RC.RP)**	**RC.RP-1:** Execute recovery plan during or after an event	P2	Establish an internal and external communication plan as part of the DDoS run book that is used every time there is a DDoS incident
	Communications (RC.CO)	**RC.CO-1:** Manage public relations	P2	Ensure impacted applications are restored and availability communicated to relevant stakeholders Manage external communications based on visibility and impact of the DDoS attack on customers, partners or public