

Function	Category	Subcategory
	<p>Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.</p>	<p>ID.AM-1: Physical devices and systems within the organization are inventoried</p>
		<p>ID.AM-2: Software platforms and applications within the organization are inventoried</p>
		<p>ID.AM-3: Organizational communication and data flows are mapped</p>
		<p>ID.AM-4: External information systems are catalogued</p>
		<p>ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value</p>
	<p>Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles</p>	<p>ID.BE-4: Dependencies and critical functions for delivery of critical services are established</p> <p>ID.BE-5: Resilience requirements to support delivery of critical</p>

IDENTIFY (ID)	<p>cybersecurity roles, responsibilities, and risk management decisions.</p>	<p>services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)</p>
	<p>Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.</p>	<p>ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed</p>
	<p>Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>ID.RA-1: Asset vulnerabilities are identified and documented</p>
		<p>ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources</p>
		<p>ID.RA-3: Threats, both internal and external, are identified and documented</p>
		<p>ID.RA-4: Potential business impacts and likelihoods are identified</p>
		<p>ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk</p>
		<p>ID.RA-6: Risk responses are identified and prioritized</p>

	<p>Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p>ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders</p>
		<p>ID.RM-2: Organizational risk tolerance is determined and clearly expressed</p>
		<p>ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis</p>
	<p>Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.</p>	<p>ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders</p>
		<p>ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process</p>
		<p>ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.</p>
<p>ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.</p>		
<p>ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers</p>		
		<p>PR.AC-1: Identities and credentials</p>

	<p>Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</p>	<p>are issued, managed, verified, revoked, and audited for authorized devices, users and processes</p>
		<p>PR.AC-2: Physical access to assets is managed and protected</p>
		<p>PR.AC-3: Remote access is managed</p>
		<p>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties</p>
		<p>PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)</p>
		<p>PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions</p>
		<p>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)</p>
	<p>PR.AT-1: All users are informed and trained</p>	

Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

PR.AT-2: Privileged users understand their roles and responsibilities

PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities

PR.AT-4: Senior executives understand their roles and responsibilities

PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities

Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.

PR.DS-1: Data-at-rest is protected

PR.DS-2: Data-in-transit is protected

PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition

PR.DS-4: Adequate capacity to ensure availability is maintained

PR.DS-5: Protections against data

PROTECT (PR)

PR.DS-5: Protections against data leaks are implemented

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity

PR.DS-7: The development and testing environment(s) are separate from the production environment

PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

PR.IP-2: A System Development Life Cycle to manage systems is implemented

PR.IP-3: Configuration change control processes are in place

PR.IP-4: Backups of information are conducted, maintained, and tested

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met

PR.IP-6: Data is destroyed according to policy

PR.IP-7: Protection processes are improved

PR.IP-8: Effectiveness of protection technologies is shared

PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

PR.IP-10: Response and recovery plans are tested

PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)

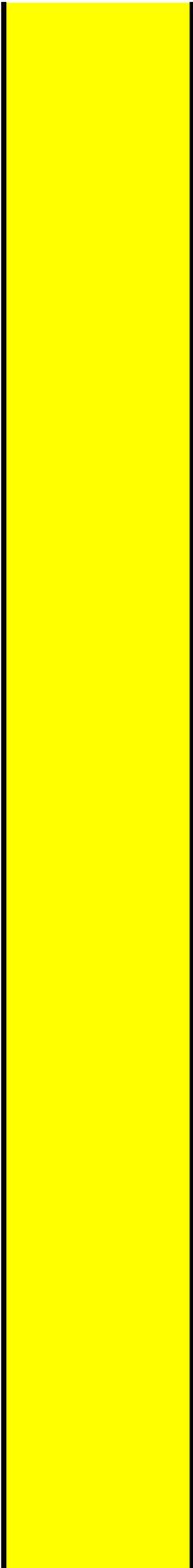
PR.IP-12: A vulnerability management plan is developed and implemented

Maintenance (PR.MA): Maintenance and repairs of industrial control and information system

PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools

	<p>components are performed consistent with policies and procedures.</p>	<p>PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access</p>
	<p>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</p>
		<p>PR.PT-2: Removable media is protected and its use restricted according to policy</p>
		<p>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities</p>
		<p>PR.PT-4: Communications and control networks are protected</p>
		<p>PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations</p>
	<p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed</p>	
	<p>DE.AE-2: Detected events are analyzed to understand attack targets and methods</p>	

DETECT (DE)	<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors
		DE.AE-4: Impact of events is determined
		DE.AE-5: Incident alert thresholds are established
	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	DE.CM-1: The network is monitored to detect potential cybersecurity events
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
	DE.CM-4: Malicious code is detected	



	DE.CM-5: Unauthorized mobile code is detected
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
	DE.CM-8: Vulnerability scans are performed
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
	DE.DP-2: Detection activities comply with all applicable requirements
	DE.DP-3: Detection processes are tested
	DE.DP-4: Event detection information is communicated

		<p>DE.DP-5: Detection processes are continuously improved</p>
	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	<p>RS.RP-1: Response plan is executed during or after an incident</p>
	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	<p>RS.CO-1: Personnel know their roles and order of operations when a response is needed</p>
		<p>RS.CO-2: Incidents are reported consistent with established criteria</p>
		<p>RS.CO-3: Information is shared consistent with response plans</p>
		<p>RS.CO-4: Coordination with stakeholders occurs consistent with response plans</p>
		<p>RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness</p>
		<p>RS.AN-1: Notifications from detection systems are investigated</p>

RESPOND (RS)

Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.

RS.AN-2: The impact of the incident is understood

RS.AN-3: Forensics are performed

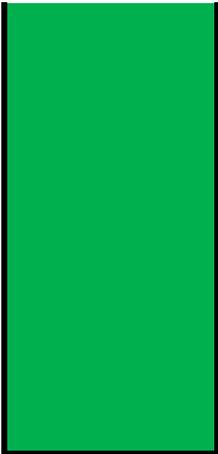
RS.AN-4: Incidents are categorized consistent with response plans

RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

RS.MI-1: Incidents are contained

Mitigation (RS.MI):

	<p>Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</p>	<p>RS.MI-2: Incidents are mitigated</p>
		<p>RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks</p>
	<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	<p>RS.IM-1: Response plans incorporate lessons learned</p>
		<p>RS.IM-2: Response strategies are updated</p>
	<p>Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents</p>	<p>RC.RP-1: Recovery plan is executed during or after a cybersecurity incident</p>
	<p>Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.</p>	<p>RC.IM-1: Recovery plans incorporate lessons learned</p> <p>RC.IM-2: Recovery strategies are updated</p>
RECOVER (RC)		

	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	RC.CO-1: Public relations are managed
		RC.CO-2: Reputation is repaired after an incident
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

Comment

Priority: 1

Catalog critical Internet facing services by location and capacity

Catalog ISP connectivity by ISP, bandwidth usage, bandwidth available

Priority: 1

Determine critical Internet facing services by type of application/service, IP address and hostname, and

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

Priority: 3

Identify applications and services that are run in cloud, SaaS, hosting or other

Priority: 2

Determine what Internet facing services will result in the most business impact if they were to become unavailable

Priority: 2

Catalog external dependencies for services and applications including DNS, NTP, cloud/hosting provider,

Priority: 3

Ensure geographical redundancy and high availability of equipment providing services, network infrastructure and Internet

Priority: 1

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

Priority: 2

Determine network and application bottlenecks including throughput, connection rate and total connections

Priority: 3

Monitor vulnerabilities lists (CVE, NVD and similar) to check if critical Internet facing services have vulnerabilities that

Priority: 3

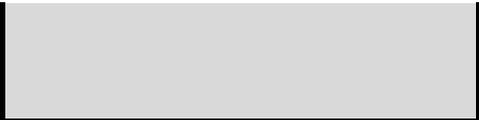
Continuously gather industry information around DDoS trends, peak attack sizes, frequency, targeted

Priority: 2

Create a risk profile that quantifies potential cost of recovery operations per DDoS incident, revenue loss,



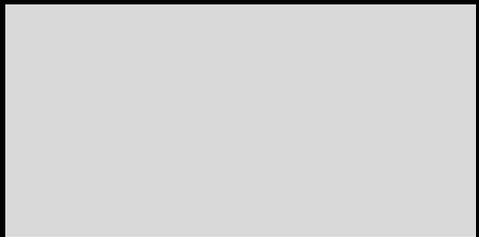
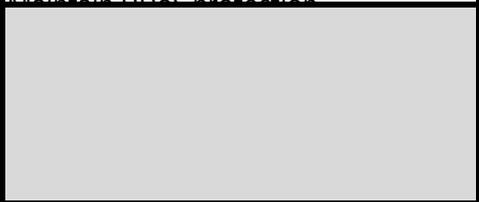
Priority: 1



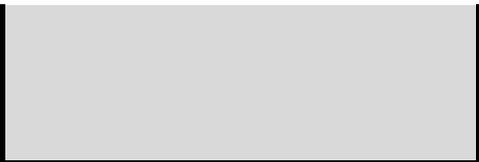
Priority: 1

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

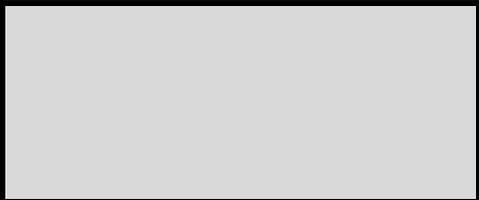


Priority: 2 Conduct a minimum of 2 annual tests of DDoS protection capabilities Perform after-action reviews following all DDoS incidents and DDoS protection tests adjusting DDoS
Priority: 3 The organization's Business Continuity and Disaster Recovery plans should have components to address the
Priority: 3 The DDoS components of the Business Continuity and Disaster Recovery plans should be tested.
Priority: 3 Vulnerabilities that can be leveraged for DDoS events should be



Priority: 1

Perform filtering of traffic to control network and/or control plane traffic policing



Priority: 1

Continuously measure traffic to hosts, resources or groups of resources to determine expected traffic over time.

Determine traffic baselines at IP layers 3 and 4 including IP bandwidth, TCP, UDP, ICMP, GRE, and at the application level including critical applications such

Priority: 1

Determine source and destination traffic characteristics when anomalous

traffic is detected that is indicative of DDoS

Priority: 2

Aggregate data for detected DDoS events from multiple network sources contributing to the attack.

Priority: 2

Total traffic rates for DDoS events can be measured across all contributing network sources

Performance and availability of services can be measured before,

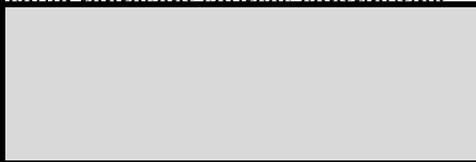
Priority: 1

Configure notifications to security monitoring personnel and appropriate

Priority: 1

Continuously measure traffic install network ingress points and between transit points on the internal network for traffic anomalies

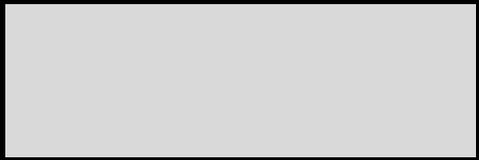
To the extent possible and/or practical from a business perspective, continually measure outbound traffic for detection of traffic anomalies that could represent sources contributing





Priority: 1

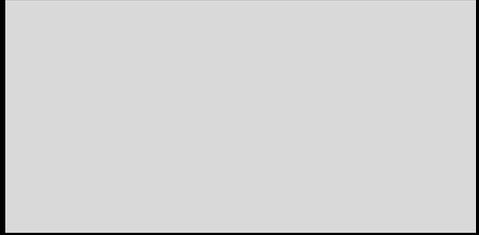
Scan Internet facing services and software applications to identify vulnerabilities that can be exploited



Priority: 2

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



Priority: 2

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,

Priority: 1

Follow DDoS response run book during any detected DDoS events

Priority: 1

Define personnel responsible for detection, mitigation, coordination and communication during DDoS



Priority: 1

Document operational run book that includes roles, responsibilities and escalation process for all parties responsible for DDoS incident response including internal personnel

Priority: 3

Share and receive DDoS attack trends with consultants, service companies and/or threat intel entities to keep abreast of attack scale, frequency,

Priority: 1

Add DDoS alert notifications to monitoring and response systems including security and network operations management systems

Priority: 2

Compare DDoS traffic rates, connection rates and total connections against documented system and network limits

Priority: 3

Save raw anomaly details in available form (logs, packet captures, flow telemetry data) to investigate parties involved in the incident and, where

Priority: 2

Implement a process or processes to analyze and respond to vulnerability information related to at-risk systems, received from internal testing, security bulletins, or security researchers

Priority: 1

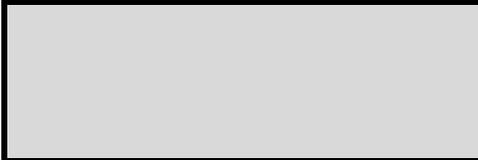
Mitigate DDoS attacks using any or all of the following:

- 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

- 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



Priority: 2

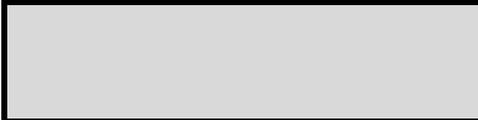
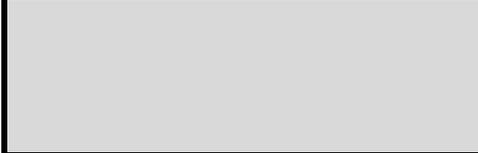
Adjust mitigation processes, capacity, technology and partnerships based on DDoS attack trends, DDoS response testing and results of DDoS after-action reviews

Maintain key security metrics around



Priority: 2

Establish an internal and external communication plan as part of the DDoS run book that is used every time there is a DDoS incident



Priority: 2

Ensure impacted applications are

Ensure impacted applications are restored and availability communicated to relevant stakeholders

Manage external communications

