[redacted]
To: cyberframework
[redacted]
Subject: RE: Discussion Draft | NIST Cybersecurity Framework 2.0 Core
Date: Monday, May 29, 2023 5:29:45 PM

NIST CSF Team,

Thanks for this opportunity to provide feedback on v2.0. The discussion draft is well-written. Here is my response to your request for feedback.

I. High-level feedback:

- **New Subcategories**

It's healthy to be skeptical about new subcategory entries. NIST CSF v1.1 is elegant due to the moderate number of controls. Any new controls should necessary, clearly identifying or mitigating risk.

- Consider whether each new subcategory is necessary.
  - Why is this new requirement needed?
  - How will it identify or mitigate risk in a way not addressed by an existing requirement?
  - Could this entry be used as an implementation example instead?
  - Candidates for evaluation: PR.PS-06, RS.MA-05 and RS.AN-08
- Be thoughtful and deliberate when providing a list within a subcategory.
  - Each list entry is a mini-requirement that must be interpreted and adhered to.
  - e.g. GV.RM-06: Responsibility and accountability are determined and communicated for ensuring that the risk management strategy and program are **(1)** resourced, **(2)** implemented, **(3)** assessed, and **(4)** maintained
- New subcategories should not be added for management routines within an existing subcategory.
  - The subcategory should be in place and effective. Management should determine how that happens.
  - Candidates for evaluation: GV.RM-07, PR.PS-03 and RS.MA-05
- New subcategories increase compliance burden. None of them should be "nice to have".
  - Adoption will decrease if the CSF becomes overly prescriptive.
  - I know it's difficult to maintain the balance.

- **Crosswalk and Mappings**

- It would be helpful to have CSF mappings to
  - PCI DSS v4.0
  - NIST Privacy Framework v1.0

II. Detailed feedback:

1. CSF 2.0 Subcategories

- **GV.PO-02: The same policies used internally are applied to suppliers**

- Suppliers do not have the capacity to review and adhere to the policies of each of their

customers unfortunately.
- Therefore, this requirement would be red-lined within most contracts.
- Try something flexible such as "Suppliers adhere to reputable practices such as the NIST cybersecurity framework or ISO 27001".

• **[NEW] PR.DS-##: Storage and use of sensitive data is kept to a minimum**
- Example 1: Sensitive unique identifiers such as Social Security Numbers are replaced with a customer number.
- Example 2: Payment card numbers are tokenized, reducing risk, compliance burden and control cost.
- Example 3: Social Security Numbers are masked in the application, with only the last 4 digits visible.
- Example 4: Payment card numbers are truncated in the database, only the first 6 and last 4 numbers are stored.
- Example 5: Exposure duration is limited, sensitive data is deleted immediately after the task completes.

• **[NEW] PR.DS-##: Specialized controls protect highly sensitive data**
- Example 1: Data categories are assigned CIA ratings mapped to a control framework. Corresponding controls are implemented where data is stored, processed or transmitted.
- Example 2: The cybersecurity program maintains controls specific to line of business products, services and assets.
- Example 3: A second person is required to sign-off on all fund disbursements before a payment can be made (two-person integrity).
- Example 4: An air gap is used to restrict network access to research data.
- Example 5: The cybersecurity program accounts for intersections with privacy management and fraud prevention programs.

• **[NEW] DE.CM-##: Highly sensitive and valuable data is monitored for suspicious activity**
- Example 1: Enhanced monitoring has been implemented for privileged users such as finance personnel with the ability to manage funds.
- Example 2: Searches for unstructured data are conducted such as PII on laptops, servers, network file shares, SharePoint and in non-production environments.
- Example 3: Dark web monitoring searches for company data such as login passwords or pre-attack adversarial activity.

2. CSF 2.0 Implementation Examples

Thanks for adding implementation examples to the framework! Here are my recommendations to help clarify the one sentence control requirements:

• **ID.RA-01:**
- ~~Example 1: Vulnerability scans are performed to identify unpatched and misconfigured software~~
- Example 1: Infrastructure vulnerability scans evaluate internal and Internet-exposed systems.
- Example #: Infrastructure vulnerability scans evaluate systems from the network (unauthenticated) and within operating systems (authenticated).
- Example #: Infrastructure is evaluated by penetration testing where sensitive data is present.
- Example #: Security benchmark dashboards are reviewed monthly (e.g. Microsoft Secure Score

and AWS Trusted Advisor).
- ~~Example 4: Software developed by the organization is reviewed, analyzed, or tested to identify vulnerabilities~~
- Example 4: All web applications are subjected to source code scanning and software composition analysis.
- Example #: Applications that store, process or transmit sensitive information are also tested with dynamic application scanning.
- Example #: Internet-exposed applications that host sensitive data are also subjected to web application penetration testing.

• GV.OC-04:
- Example 1: IT functions that provide or materially support critical services are documented within a Disaster Recovery Plan.
- Example 2: Detailed procedures are in place for continuing to provide critical business services during an outage, natural disaster or attack such as denial of service or ransomware.
- Example 3: Recovery plans enable service restoration within Recovery Time Objectives.

• GV.OC-05:
- Example 1: Business functions that provide or materially support critical services are documented within Business Continuity Plans.

• GV.RM-02:
- Example 1: A Third Party Risk Management Program addresses suppliers, vendors and service providers.

• GV.RM-04:
- Example 1: A risk register process provides transparency to senior executives and the board of directors.
- Example 2: Risk management meetings include a focus on the threat landscape and operational risk.

• GV.RM-05:
- Example 1: Risk issues are prioritized by severity and communicated to the appropriate tier of leadership.
- Example 2: Risk decisions are documented in meeting minutes and within a system of record.
- Example 3: Risk acceptance are instances of low risk and high cost of remediation or vulnerabilities that cannot be remediated, with compensating controls to the extent possible.

• GV.RM-06:
- Example 1: Risk management roles and responsibilities are documented within a policy.
- Example 2: Risk management responsibilities are documented within job descriptions.
- Example 3: Risk management responsibilities are communicated within awareness and training activities.

• GV.RM-08:
- Example 1: Senior executives receive risk transparency through reporting, metrics and meeting routines. Details of assessments, scans and remediation is provided.
- Example 2: The CEO and the Board of Directors are briefed on cybersecurity assessments, penetration tests and remediation of cybersecurity issues.
- Example 3: Cybersecurity reporting, metrics, KPIs and KRIs feed into an Enterprise Risk Management program.
- Example 4: Adherence to remediation policy is monitored within vulnerability management

metrics.

• **GV.RR-01:**

- Example 1: Operational functions and lines of business are required to declare self-identified audit issues, with metrics in place to demonstrate the control environment is improving continuously.

• **GV.RR-02:**

- Example 1: Policy provides clear direction of what employees must do to protect the organization from cybersecurity threats and vulnerabilities.
- Example 2: Cybersecurity responsibilities within operations, risk functions and internal audit are clearly articulated.
- Example 3: Cybersecurity professionals are assigned to review and respond to alerts, monitoring reports and dashboards.
- Example 4: Responsibilities for each sub-category are designated within a RACI matrix (responsible, accountable, consulted and informed).

• **GV.RR-04:**

- Example 1: Default contract language requires third parties to adhere to reputable practices such as the NIST cybersecurity framework or ISO 27001.
- Example 2: The customer has the right to audit the vendor, related services, and IT controls from a cybersecurity perspective.
- Example 3: Immediate notification is required if a security incident is suspected or known to be taking place.
- Example 4: Upon contract termination, vendor agrees to return and destruction of data.
- Example 5: The cybersecurity team reviews IT service contracts and evaluates proposed redlines to contract language.

• **GV.RR-05:**

- Example 1: There is appropriate separation of duties in the CISO's reporting structure, such as reporting to the CEO, Chief Risk Officer or Board of Directors. When the CISO reports to the CIO/CTO, it is a conflict of interest.
- Example 2: The CISO provides triannual updates to the Board of Directors or similar executive group.
- Example 3: A Communications Plan details awareness and risk transparency exchanges with employees, contractors, management, internal audit and the board of directors.

• **GV.RR-06:**

- Example 1: Capacity to execute on core cybersecurity processes is evaluated every two years.
- Example 2: A Primary and Alternate Duties List is used to determine if the average number of primary duties assigned to employees is reasonable, if roles should be further distributed or if additional staffing is warranted.

• **GV.RR-07:**

- Example 1: Human resources conducts background checks prior to onboarding new personnel.
- Example 2: HR notifies Identity and Access Management when personnel start with the organization, change roles or leave the organization.
- Example 3: HR notifies the cybersecurity team when an employee exhibits insider threat behavioral indicators.

• **GV.PO-01:**

- Example 1: Employees acknowledge receipt of policies when first hired, annually and any time a

policy is updated.
- Example 2: Business and operations services are documented within process diagrams.
- Example 3: Process diagrams include swim lanes, critical control points and references to procedures.
- Example 4: Procedures manuals are in place for business and operational functions.

• **GV.PO-03:**
- Example 1: Policies, process diagrams and procedures manuals are reviewed and updated at least annually.
- Example 2: Process diagrams are subjected to risk evaluation such as Failure Modes and Effects Analysis.
- Example 3: Risk evaluation occurs when a process is created and every three years thereafter.

• **ID.AM-01:**
- Example 1: An inventory documents systems and devices within the organization's span of control (workstations, servers, network devices, mobile devices, etc.).
- Example 2: An active discovery tool identifies devices connected to the network and updates the inventory automatically.
- Example 3: Operational Technology (OT) and Internet of Things (IoT) devices are in scope for the inventory.

• **ID.AM-02:**
- Example 1: An inventory documents Commercial Off-the-Shelf (COTS) software installed on the organization's systems.
- Example 2: An inventory documents custom application software developed by the organization or by a vendor on the organization's behalf.
- Example 3: Vendor hosted Software as a Service (SaaS) applications are included within the inventory.

• **ID.AM-05:**
- Example 1: Resources are labeled based on classification such as Restricted, Confidential, Internal and Public.
- Example 2: A business criticality rating is assigned to each system and application within the inventory.

• **ID.AM-07:**
- Example 1: System and software inventories include sensitive data categories such as Personally Identifiable Information (PII), Protected Health Information (PHI) and intellectual property**.**

• **ID.AM-08:**
- Example 1: Data is sanitized by shredding physical media such as a hard drive or by overwriting the data three times with a software program.
- Example 2: Remote maintenance is conducted with an internally issued laptop to ensure appropriate security configurations and software are in place.
- Example 3: Remote access is restricted to only the networks, systems and applications required to conduct maintenance.

• **ID.RA-02:**
- Example 1: Cybersecurity professionals receive cyber threat intelligence from reputable sources (e.g. CISA, InfraGard and an Information Sharing and Analysis Center (ISAC)).
- Example 2: Software is configured to receive updated threat information (e.g. endpoint protection and response, vulnerability scanning tools, etc.).

- Example 3: Security Information and Event Management (SIEM) software ingests cyber threat intelligence feeds.

• **ID.RA-03:**

- Example 1: An analysis of in-scope threat actors for the organization has been documented.
- Example 2: The analysis includes a description of their motivations and targeted data.
- Example 3: Nation states, criminal enterprises, insider threat and hacktivists are considered within the analysis.
- Example 4: Risk assessments include newly adopted technologies such as Generative AI.

• **ID.RA-05:**

- Example 1: Assessment scope includes key systems and applications that would likely be of risk based on threat actors, their motivations and targeted data.
- Example 2: The assessment documents technical security weaknesses that could be exploited by identified threat actors, resulting in business impact.

• **ID.RA-06:**

- Example 1: Vulnerabilities are remediated and tracked to closure based on risk priority.
- Example 2: CISA Known Exploited Vulnerabilities are considered high risk, to be remediated within one week.
- Example 3: Responses include compensating controls to mitigate risk, aligned with the organization's risk tolerance.
- Example 4: Plan of Action and Milestones (POA&Ms) are documented based on findings from security control assessments and continuous monitoring activities.
- Example 5: Risk register entries document extended remediation (risk mitigate) or instances when a vulnerability will be left in place (risk accept).

• **ID.RA-07:**

- Example 1: Change request tickets include fail-back plans. Testing is conducted in a non-production environment.
- Example 2: Change requests are submitted for approval to a Change Advisory Board (CAB) or similar function.
- Example 3: Changes are implemented within a maintenance window, with testing to ensure functionality has not been adversely affected.
- Example 4: Cybersecurity representatives are assigned to the CAB (primary and alternate).

• **ID.RA-08:**

- Example 1: Prospective suppliers and service providers are evaluated through procurement processes.
- Example 2: IT equipment is purchased though reputable manufacturers and resellers to minimize supply chain risk.
- Example 3: Commercial services are used to validate the legitimacy and financial solvency of a prospective suppler (e.g. Thomson Reuters and Dun & Bradstreet).

• **ID.RA-09:**

- Example 1: Cyber threat intelligence drives activities such as installing a patch or implementing a security configuration.
- Example 2: Cybersecurity professionals conduct threat hunts, actively searching for adversaries in the IT environment.
- Example 3: Threat intelligence and hunting activities are documented in a log or service desk tickets.

• **ID.RA-10:**
- Example 1: Low risk exceptions to security policies or standards are documented within a Policy Exception Request Form.
- Example 2: Exceptions that will eventually meet the requirement are documented in a Plan of Action and Milestone (POA&M).
- Example 3: Moderate or high risk exceptions are documented within a risk register entry.

• **ID.SC-03:**
- Example 1: Default contract language mandates supplier and service provider adherence to a reputable cybersecurity control framework.
- Example 2: The legal department must consult the cybersecurity team when a supplier asks to redline contract security language.
- Example 3: The cybersecurity team must be engaged to review IT service contracts.

• **ID.SC-04:**
- Example 1: A risk rating is established for each supplier and third party provider based on data sensitivity and business criticality.
- Example 2: Criteria is established for how each supplier will be evaluated (e.g. independent assessment, questionnaire with artifacts, vulnerability scans, etc.).

• **ID.SC-06:**
- Example 1: Supplier termination processes confirm that user and service accounts have been deactivated.
- Example 2: The supplier provides customer's information in a mutually acceptable format.
- Example 3: Customer information is securely deleted within service provider systems. Printed customer information is shredded.

• **ID.IM-01:**
- Example 1: A cybersecurity program assessment occurs every three years.
- Example 2: The assessment is conducted by an independent internal function separate from operations or an external firm.
- Example 3: The assessment is based upon a reputable cybersecurity control framework.
- Example 4: The assessment considers the threat landscape, likely adversaries, sensitive data, attack techniques and in-place controls.
- Example 5: Line of Business assessments evaluate critical processes, where sensitive data is stored, processed and transmitted.
- Example 6: Targeted cybersecurity assessments are conducted such as DevSecOps, Security Operations Center (SOC), ransomware preparedness and insider threat.

• **ID.IM-02:**
- Example 1: The company participates in annual cybersecurity tabletop exercises with an Information Sharing and Analysis Center (ISAC).
- Example 2: Critical service providers that store, process or transmit sensitive data are included within incident response exercises.
- Example 3: Critical service providers are included within business continuity and disaster recovery exercises.
- Example 4: Unannounced penetration tests evaluate the response process of managed security service providers.
- Example 5: Automated monitoring determines whether technical controls are in place and effective.

• **ID.IM-03:**
- Example 1: Include a requirement for lessons learned within incident response, business continuity and disaster recovery plans.
- Example 2: Implementation of new controls to prevent reoccurrence are tracked to closure.
- Example 3: Threat intelligence and hunting drives requirements for new alerts and analysis reports.

• **PR.AA-01:**
- Example 1: The supervisor submits an access request when a new employee or contractor joins the organization.
- Example 2: The Identity and Access Management team reviews the request and grants IT resource access as appropriate for the role.
- Example 3: Requests to access sensitive information require approval from the data owner.
- Example 4: Access is rescinded on the user's last day with the organization.

• **PR.AA-02:**
- Example 1: System accounts and physical access are associated with an individual employee or contractor. Shared accounts are not permitted.
- Example 2: Privileged Access Management software is used to restrict administrative access and for enhanced logging.
- Example 3: Interactive logon to service accounts is disabled and monitored to prevent abuse.

• **PR.AA-03:**
- Example 1: Remote access to the organization's network, servers, virtual machines and applications is restricted by Multi-Factor Authentication (MFA).
- Example 2: Changes in risk profile such as impossible travel or login from a hostile nation state automatically locks the account.
- Example 3: Access to sensitive information such as PII, PHI or research data requires a second layer of MFA.
- Example 4: Remote access from the Internet is restricted by Virtual Private Network (VPN) and MFA.
- Example 5: Segmented networks that host sensitive data require additional authentication such as a jump box with MFA.
- Example 6: SaaS solutions authenticate via Single Sign-On where technically feasible.

• **PR.AA-05:**
- Example 1: Supervisors conduct access control reviews of their reports bi-annually to prevent privilege creep.
- Example 2: When an employee transitions to a new role, an access control review is conducted by the hiring manager. Legacy accesses must be rescinded within 30 days.
- Example 3: Developers do not have access to production environments. A separate role must promote code to production.
- Example 4: End users do not have administrative access to their workstations.

• **PR.AA-06:**
- Example 1: A current list of employees and contractors is compared to active directory accounts each quarter.
- Example 2: A current list of employees and contractors is compared to active ID access badges each quarter.
- Example 3: Quarterly reviews evaluate ID cards with extensive access such as computer rooms

and ‘all access’.
- Example 4: IT staff confirm hiring managers have conducted periodic access reviews and all legacy accesses have been rescinded.

• **PR.AA-07:**
- Example 1: Layered physical access controls are in place (e.g. perimeter, lobby, stairwells, office space and sensitive areas such as computer rooms).
- Example 2: Physical security controls such as locks, access card readers, alarm systems, cameras and physical security guards are used to restrict access.
- Example 3: During business hours the building lobby is staffed to authenticate and log visitors and delivery personnel.

• **PR.AT-01:**
- Example 1: Employees and contractors attend security awareness training to provide them with an understanding of threats and vulnerabilities, including necessary actions to prevent and mitigate risk.
- Example 2: Training is required upon starting with the organization and annually thereafter. A testing component ensures the trainee understands security policy and what is expected of them.
- Example 3: Phishing test messages are sent to employees and contractors each month.
- Example 4: If a user fails the test, an educational message is displayed (1st occurrence), additional training is required (2nd) and an e-mail is sent to the user, their supervisor and the awareness team (3rd).
- Example 5: Incident response team members receive training so they understand their role and are familiar with the incident response plan.

• **PR.AT-02:**
- Example 1: Specialized security awareness training is provided to system administrators and finance personnel that conduct wire transfers.
- Example 2: Training is required upon starting in those roles and annually thereafter.
- Example 3: Cybersecurity and physical security personnel are trained to ensure their skill sets keep pace with emerging threats and changes in technology.

• **PR.AT-04:**
- Example 1: Senior executives receive training on their cybersecurity responsibilities, such as promoting risk transparency.
- Example 2: Leadership training includes security responsibilities across operations, risk functions and internal audit.
- Example 3: Leaders are briefed on the need for cybersecurity controls specific to line of business products, services and assets.

• **PR.DS-01:**
- Example 1: Sensitive data-at-rest is protected using strong encryption such as AES-256.
- Example 2: Databases are protected with at least field-level encryption.
- Example 3: Use of removable media by the IT team is controlled and inventoried (e.g. backup tapes and flash drives used to install network operating systems).

• **PR.DS-02:**
- Example 1: Outbound e-mail containing 50 PII records or less is automatically encrypted by data loss prevention software.
- Example 2: Outbound e-mail containing more than 50 PII records is blocked, with notification sent to the supervisor and the SOC.

- Example 3: Outbound file transfer protocol usage is restricted to business operations traffic (e.g. FTP). Unauthorized file transfers are blocked.

• **PR.DS-09:**

- Example 1: Data is disposed of when no longer required in accordance with a data retention policy.
- Example 2: Online data is deleted when the time period has elapsed (e.g. data stored within applications).
- Example 3: Systems and physical media are decommissioned in accordance with a data destruction policy (e.g. PCs, laptops, servers, hard drives, solid-state drives and paper media).

• **PR.DS-10:**

- Example 1: End users do not have access to technology commonly used to exfiltrate data such as external storage, Internet storage and personal e-mail (e.g. USB drives, Dropbox and Gmail, respectively).

• **PR.DS-11:**

- Example 1: Backup testing of system and data occur at least annually. Database restore is included within testing.
- Example 2: Backups are retained offline to prevent a ransomware outbreak from encrypting data in backups as well.

• **PR.PS-01:**

- Example 1: Operating systems and commercial software are hardened against attack with security configurations.
- Example 2: PowerShell is hardened to make it difficult to “live off the land”.
- Example 3: Configuration monitoring software alerts when changes to security hardening configurations occur.
- Example 4: Changes are implemented within a maintenance window.
- Example 5: Testing is conducted to ensure functionality has not been adversely affected.

• **PR.PS-02:**

- Example 1: A vulnerability management plan addresses in-scope systems and applications, vulnerability scanning processes and how remediation is tracked to closure.
- Example 2: Vulnerability trend reporting and root cause analysis drives efforts to prevent reoccurring software code defects.
- Example 3: Developers implement security code such as a filter that prevents a vulnerability from being exploited.

• **PR.PS-04:**

- Example 1: Operating systems and commercial software are configured to log security events such as logins, privilege escalation, object access and changes to logs.
- Example 2: Network devices have security log configurations in place such as routers, switches, wireless access points and domain controllers.
- Example 3: Security tools have security log configurations in place such as firewalls, VPNs, IDS/IPS, endpoint protection and response, data loss prevention, web filters and honeypots.
- Example 4: Custom applications are configured to be “attack aware”, with a security logging framework such as the OWASP AppSensor project.

• **PR.PS-05:**

- Example 1: A web application firewall protects Internet-facing web applications that store, process or transmit sensitive data.

- Example 2: Allowlisting software permits authorized programs to run and blocks all others. It is used as preventive control against ransomware and other malware.
- Example 3: DNS resolution is restricted to a web content filter, which blocks access to known malicious domains and command-and-control systems.
- Example 4: Laptop web content filter and data loss prevention restrictions remain in place off network.
- Example 5: An API gateway authenticates access to applications and the data within.

• **PR.PS-07:**
- Example 1: In-scope scans and penetration tests must be conducted within sprints and before each release.
- Example 2: Software code with high or critical defects cannot be released to production.

• **PR.IR-01:**
- Example 1: The Incident Response Plan addresses common scenarios such as 'impacted by cyber intrusion', ransomware, ‘cloud hosting’, ‘service provider incident’ and ‘supplier vulnerability’.
- Example 2: Detailed playbooks and contact information are included within the Incident Response Plan.
- Example 2: Business Continuity Plans address specific response procedures for each critical business process (versus one plan for enterprise work productivity).
- Example 4: Each plan is reviewed annually and updated as appropriate.

• **PR.IR-02:**
- Example 1: Network firewall rules are configured with granular source/destination and port/protocol settings.
- Example 2: Rules that permit 'any' traffic to flow within source, destination or port/protocol are prohibited.
- Example 3: Systems are isolated with network segmentation such as demilitarized zone, extranet, common use, IoT, OT, security and sensitive information such as PII or research data.
- Example 4: Visitors connect to a guest wireless network, which only provides access to the Internet.
- Example 5: Production data is not used within testing environments unless production quality controls are in place.

• **PR.IR-03:**
- Example 1: A physical security policy provides control requirements to protect office buildings and other facilities.
- Example 2: Controls are implemented from the perimeter, into sensitive areas such as office space or computer rooms.

• **PR.IR-04:**
- Example 1: High availability components provide resilience in systems that support business critical applications (e.g. redundant hard drives, power supplies and network cards).
- Example 2: In the event Internet connectivity is lost, the ability to fail over to an alternate data center is in place.

• **DE.AE-02:**
- Example 1: SIEM monitoring software evaluates events and determines if they correspond to Indicators of Compromise (IOCs) or Tactics, Techniques, and Procedures (TTPs).
- Example 2: The SIEM populates reports and dashboards for events that require further analysis.
- Example 3: Behavioral analysis software monitors systems and users. Unusual activity is sent to

the SOC for investigation and response.

- **DE.AE-03:**

- Example 1: Operating systems, commercial software and custom applications replicate logging, events, warnings and alerts to a central repository.
- Example 2: Network devices' logs and events are monitored (routers, switches, wireless access points and domain controllers).
- Example 3: Security tools' logs and events are monitored (firewalls, VPNs, IDS/IPS, endpoint protection and response, data loss prevention, web filters and honeypots).

- **DE.AE-04:**

- Example 1: The impact of security events is initially evaluated by SIEM monitoring software.
- Example 2: Known malicious behavior results in an alert.
- Example 3: The SIEM produces a report of systems that have stopped sending log data.
- Example 4: Vulnerability scan results are accessible within a system of record.

- **DE.AE-05:**

- Example 1: Alert thresholds are configured to determine when an event is deemed to be suspicious or is confirmed to be a security issue.
- Example 2: A lateral movement alert sends notification when two systems communicate and that has not occurred within the past three months.
- Example 3: An alert sends notification when there are authentication failures across multiple accounts.
- Example 4: A role-based access alert sends notification when a Customer Service Representative accesses 30 or more PII records in an hour.

- **DE.AE-06:**

- Example 1: The SIEM sends notification of warnings, alerts and suspicious activity to the SOC for analysis.
- Example 2: SIEM alerts are integrated into the ticketing system for rapid response and accountability.
- Example 3: The help desk procedures manual provides instructions to report suspicious security events to the SOC for analysis.
- Example 4: An alert is sent when an account is added to the domain admin group.
- Example 5: If an administrative account logs in between 12:00 and 5:00, a ticket is opened and the SOC investigates.
- Example 6: An alert occurs when a system attempts to resolve DNS from the Internet versus the expected
path of the web content filter.

- **DE.AE-07:**

- Example 1: Enhanced monitoring is initiated when an employee exhibits insider threat behavioral indicators.
- Example 2: When an employee gives notice, a log review is conducted to monitor for data exfiltration.
- Example 3: Cybersecurity personnel monitor and respond to suspicious activity 24x7/365 within the SOC.
- Example 4: The SOC Manager analyzes reported security events to determine if they meet the criteria for a cybersecurity incident.

- **DE.AE-08:**

- Example 1: When the SOC Manager declares an incident, an Incident Response Coordinator (IRC) is appointed and the Incident Response Plan is initiated.
- Example 2: Automated response mitigates malicious activity such as Security Orchestration, Automation and Response (SOAR) software.
- Example 3: A data breach response service dispatches remote and on-site personnel to provide a comprehensive recovery strategy.

• **DE.CM-01:**

- Example 1: Malicious code is identified by endpoint protection using machine learning or behavioral analysis and is then blocked automatically.
- Example 2: The e-mail gateway identifies malicious code, which is then blocked automatically.
- Example 3: Security software on mobile devices prevents malicious applications from being installed and blocks access to known malicious websites.
- Example 4: Jailbroken mobile devices are blocked from connecting to the corporate network.
- Example 5: Company file attachments cannot be downloaded to mobile device storage.
- Example 6: Network Access Control (NAC) prevents rouge devices from connecting to the network (e.g. a wireless access point).

• **DE.CM-02:**

- Example 1: The physical environment is monitored with alarm systems, cameras and physical security guards.
- Example 2: Periodic reviews are conducted to ensure physical security controls are effective.
- Example 3: Physical access controls such as door locks, latches and hinge pins are evaluated for resistance to breaching tools.

• **DE.CM-03:**

- Example 1: User and Entity Behavior Analytics (UEBA) software is used by the SOC to detect suspicious activity.
- Example 2: A data exfiltration alert sends notification when a user attempts to access 3 or more of the following within 2 hours: personal e-mail, external drive storage, cloud storage, file transfer protocol and file printing.
- Example 3: Deception technology such as honeypots or honeynets are used as a decoy to detect adversaries.

• **DE.CM-06:**

- Example 1: The Third Party Risk Management team requests sanitized vulnerability scans from service providers annually.
- Example 2: Service providers with access to the internal network are monitored for scope of service and expected behavior.

• **DE.CM-09:**

- Example 1: Authenticated vulnerability scans of PCs, laptops, servers and virtual machines is conducted in accordance with the Security Content Automation Protocol (SCAP) standard.

• **RS.MA-01:**

- Example 1: When a cybersecurity incident is declared, team members follow procedures within the Incident Response Plan.

• **RS.MA-02:**

- Example 1: Security events are initially evaluated by security monitoring software. When suspicious activity is detected, a SOC analyst must review to determine if it is a false positive or a legitimate issue that warrants incident response.

• **RS.MA-03:**
- Example 1: Incident categories are included within the Incident Response Plan (e.g. cyber intrusion, ransomware, Priority 1).
- Example 2: Exercises and root cause analysis help confirm incidents are appropriately categorized during response activity.
• **RS.MA-04:**
- Example 1: The CISO ensures the impact of the incident is understood by engaging senior executives, line of business leaders, information technology, legal and public relations.
• **RS.AN-03:**
- Example 1: Preservation of forensic evidence and forensic investigation is included within the Incident Response Plan.
- Example 2: Forensic software and trained personnel are in place (either in-house or through a service provider).
• **RS.AN-06:**
- Example 1: Exercises and root cause analysis help confirm forensics are performed within incident response activity.
• **RS.AN-07:**
- Example 1: Forensic response team members receive training on evidence preservation and chain-of-custody.
- Example 2: Evidence preservation and chain-of-custody instructions are detailed within a procedures manual.
• **RS.AN-09:**
- Example 1: Incident status is communicated by an e-mail distribution group or a SharePoint site with alert subscriptions.
- Example 2: Status update messages include: “Information conveyed in this message contains preliminary details, what is known now. Additional information will become available as further investigation is conducted.”
• **RS.CO-02:**
- Example 1: Incident response team members keep a log of response activities with time stamps to support accurate incident reporting.
- Example 2: The Incident Response Plan contains criteria to engage the Crisis Management team.
- Example 3: The Crisis Management team maintains a listing of external stakeholders established by analysis of laws, regulations and contractual obligations.
• **RS.CO-03:**
- Example 1: When a crisis event is declared, team members follow procedures within the Crisis Communications Plan.
• **RS.CO-04:**
- Example 1: The CISO keeps senior leadership and internal stakeholders updated periodically throughout response efforts.
• **RS.CO-05:**
- Example 1: The cybersecurity team participates in an Information Sharing and Analysis Center (ISAC) for its industry.
- Example 2: Cybersecurity employees attend local InfraGard meetings.
• **RS.MI-01:**
- Example 1: A containment phase is included within the Incident Response Plan.

- Example 2: Exercises and root cause analysis help confirm incidents are contained in practice.

• **RS.MI-02:**

- Example 1: An eradication and recovery phase is included within the Incident Response Plan.
- Example 2: Exercises and root cause analysis help confirm eradication and recovery are contained in practice.

• **RC.RP-01:**

- Example 1: When a disaster is declared, team members follow procedures within the Business Continuity Plan.

• **RC.CO-01:**

- Example 1: Holding statement templates are used to initially contact external stakeholders, often by a press release. The message conveys an overview such as a data breach has occurred, an active investigation is underway and updates will be provided as more information becomes available.
- Example 2: As more information is known, additional communications are sent such as customer notifications and a letter to the attorney general.

NIST Team: Thanks so much for your efforts to protect our country! Feel free to reach out to me with questions or comments.

Gideon

Gideon T. Rasmussen | CISSP, CRISC, CISA, CISM, CIPP | Consultant
Virtual CSO, LLC | [redacted]