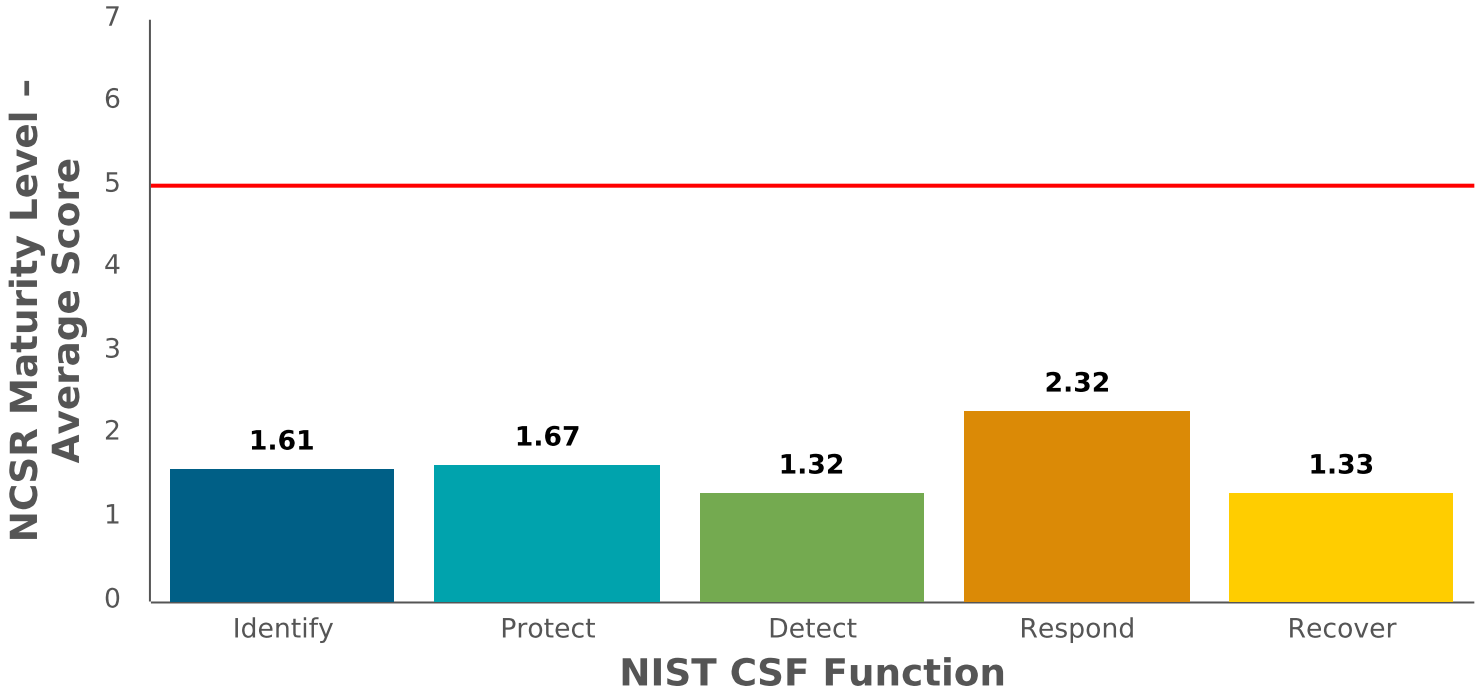
Current NCSR Results



The red line indicates an average score of 5, which is designated as the recommended minimum maturity level

Question	Response	Numerical Score
Identify		**1.61**
ID.AM		**1.83**
ID.AM-1: Physical devices and systems within the organization are inventoried.	Informally Done	2.00
ID.AM-2: Software platforms and applications within the organization are inventoried	Informally Done	2.00
ID.AM-3: Organizational communication and data flows are mapped	Not Performed	1.00
ID.AM-4: External information systems are catalogued	Informally Done	2.00
ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	Informally Done	2.00
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Informally Done	2.00
ID.BE		**1.60**
ID.BE-1: The organization's role in the supply chain is identified and communicated	Not Performed	1.00
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Informally Done	2.00

Jan 13, 2022 4:57 PM

Question	Response	Numerical Score
Identify		**1.61**
ID.BE		**1.60**
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Informally Done	2.00
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Informally Done	2.00
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Not Performed	1.00
ID.GV		**2.00**
ID.GV-1: Organizational information security policy is established and communicated	Informally Done	2.00
ID.GV-2: Cybersecurity roles & responsibilities are coordinated and aligned with internal roles and external partners	Informally Done	2.00
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Informally Done	2.00
ID.GV-4: Governance and risk management processes address cybersecurity risks	Informally Done	2.00
ID.RA		**1.67**
ID.RA-1: Asset vulnerabilities are identified and documented	Documented Policy	3.00
ID.RA-2: Cyber threat and vulnerability information is received from information sharing forums and sources	Informally Done	2.00
ID.RA-3: Threats, both internal and external, are identified and documented	Informally Done	2.00
ID.RA-4: Potential business impacts and likelihoods are identified	Not Performed	1.00
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Not Performed	1.00
ID.RA-6: Risk responses are identified and prioritized	Not Performed	1.00
ID.RM		**1.33**
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Informally Done	2.00
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	Not Performed	1.00
ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	Not Performed	1.00

Question	Response	Numerical Score
Identify		**1.61**
ID.SC		**1.20**
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Not Performed	1.00
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	Not Performed	1.00
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	Informally Done	2.00
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	Not Performed	1.00
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	Not Performed	1.00
Protect		**1.67**
PR.AC		**1.86**
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Informally Done	2.00
PR.AC-2: Physical access to assets is managed and protected	Informally Done	2.00
PR.AC-3: Remote access is managed	Informally Done	2.00
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Informally Done	2.00
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Informally Done	2.00
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	Not Performed	1.00
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organization risks)	Informally Done	2.00
PR.AT		**1.80**
PR.AT-1: All users are informed and trained	Not Performed	1.00
PR.AT-2: Privileged users understand roles & responsibilities	Informally Done	2.00

Question	Response	Numerical Score
Protect		**1.67**
PR.AT		**1.80**
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Informally Done	2.00
PR.AT-4: Senior executives understand roles & responsibilities	Informally Done	2.00

Question	Response	Numerical Score
Protect		**1.67**
PR.AT		**1.80**
PR.AT-5: Physical and information security personnel understand roles & responsibilities	Informally Done	2.00
PR.DS		**1.50**
PR.DS-1: Data-at-rest is protected	Informally Done	2.00
PR.DS-2: Data-in-transit is protected	Informally Done	2.00
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Informally Done	2.00
PR.DS-4: Adequate capacity to ensure availability is maintained	Not Performed	1.00
PR.DS-5: Protections against data leaks are implemented	Informally Done	2.00
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Not Performed	1.00
PR.DS-7: The development and testing environment(s) are separate from the production environment	Not Performed	1.00
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	Not Performed	1.00
PR.IP		**1.75**
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)	Not Performed	1.00
PR.IP-2: A System Development Life Cycle to manage systems is implemented	Informally Done	2.00
PR.IP-3: Configuration change control processes are in place	Not Performed	1.00
PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Informally Done	2.00
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	Not Performed	1.00
PR.IP-6: Data is destroyed according to policy	Informally Done	2.00
PR.IP-7: Protection processes are improved	Informally Done	2.00
PR.IP-8: Effectiveness of protection technologies is shared	Informally Done	2.00
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Partially Documented Standards and/or Procedures	4.00
PR.IP-10: Response and recovery plans are tested	Not Performed	1.00
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Not Performed	1.00

Question	Response	Numerical Score
Protect		**1.67**
PR.IP		**1.75**
PR.IP-12: A vulnerability management plan is developed and implemented	Informally Done	2.00
PR.MA		**1.50**
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	Informally Done	2.00
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Not Performed	1.00
PR.PT		**1.60**
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Not Performed	1.00
PR.PT-2: Removable media is protected and its use restricted according to policy	Not Performed	1.00
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Informally Done	2.00
PR.PT-4: Communications and control networks are protected	Informally Done	2.00
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Informally Done	2.00
Detect		**1.32**
DE.AE		**1.20**
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Not Performed	1.00
DE.AE-2: Detected events are analyzed to understand attack targets and methods	Informally Done	2.00
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	Not Performed	1.00
DE.AE-4: Impact of events is determined	Not Performed	1.00
DE.AE-5: Incident alert thresholds are established	Not Performed	1.00
DE.CM		**1.75**
DE.CM-1: The network is monitored to detect potential cybersecurity events	Informally Done	2.00
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Informally Done	2.00
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Informally Done	2.00
DE.CM-4: Malicious code is detected	Informally Done	2.00

Question	Response	Numerical Score
Detect		**1.32**
DE.CM		**1.75**
DE.CM-5: Unauthorized mobile code is detected	Not Performed	1.00
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Not Performed	1.00
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Informally Done	2.00

Question	Response	Numerical Score
Detect		**1.32**
DE.CM		**1.75**
DE.CM-8: Vulnerability scans are performed	Informally Done	2.00
DE.DP		**1.00**
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	Not Performed	1.00
DE.DP-2: Detection activities comply with all applicable requirements	Not Performed	1.00
DE.DP-3: Detection processes are tested	Not Performed	1.00
DE.DP-4: Event detection information is communicated to appropriate parties	Not Performed	1.00
DE.DP-5: Detection processes are continuously improved	Not Performed	1.00
Respond		**2.32**
RS.AN		**1.60**
RS.AN-1: Notifications from detection systems are investigated	Informally Done	2.00
RS.AN-2: The impact of the incident is understood	Informally Done	2.00
RS.AN-3: Forensics are performed	Informally Done	2.00
RS.AN-4: Incidents are categorized consistent with response plans	Not Performed	1.00
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)	Not Performed	1.00
RS.CO		**3.00**
RS.CO-1: Personnel know their roles and order of operations when a response is needed	Documented Policy	3.00
RS.CO-2: Incidents are reported consistent with established criteria	Partially Documented Standards and/or Procedures	4.00
RS.CO-3: Information is shared consistent with response plans	Partially Documented Standards and/or Procedures	4.00
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Documented Policy	3.00
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Not Performed	1.00
RS.IM		**1.00**
RS.IM-1: Response plans incorporate lessons learned	Not Performed	1.00
RS.IM-2: Response strategies are updated	Not Performed	1.00
RS.MI		**2.00**
RS.MI-1: Incidents are contained	Informally Done	2.00
RS.MI-2: Incidents are mitigated	Informally Done	2.00

Question	Response	Numerical Score
Respond		**2.32**
RS.MI		**2.00**
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Informally Done	2.00
RS.RP		**4.00**
RS.RP-1: Response plan is executed during or after an event	Partially Documented Standards and/or Procedures	4.00
Recover		**1.33**
RC.CO		**2.00**
RC.CO-1: Public relations are managed	Informally Done	2.00
RC.CO-2: Reputation is repaired after an incident	Informally Done	2.00
RC.CO-3: Recovery activities are communicated to internal and external stakeholders and executive and management teams	Informally Done	2.00
RC.IM		**1.00**
RC.IM-1: Recovery plans incorporate lessons learned	Not Performed	1.00
RC.IM-2: Recovery strategies are updated	Not Performed	1.00
RC.RP		**1.00**
RC.RP-1: Recovery plan is executed during or after a cybersecurity event	Not Performed	1.00