cerium networks®

Oregon Secretary of State

Information Security Risk Assessment

Stuart Chontos-Gilchrist, Senior Security Consultant

May 6, 2019

Scope – NIST CSF

- Managerial and Operational IT controls review (NIST Cyber Security Assessment)
- Interviewed Key Staff
- Reviewed 100+ Documents and Artifacts

Scope – Internal Technical

- Nmap Discovery Scans
- Internal Vuln Scanning Using Security Center Nessus
  - Non-Priv Scans
  - Priv Scans
- Oracle 11G CIS Review
- VMWare vSphere CIS Review
- CheckPoint Firewall Review
- Web Content Filtering Review

Scope - Web Application Testing

- Web Application Testing on Two SOS Applications – OBR and OARD
- Use OWASPv4 Auditing guidelines
- Validation of Monitoring

Scope - Physical Security Assessment

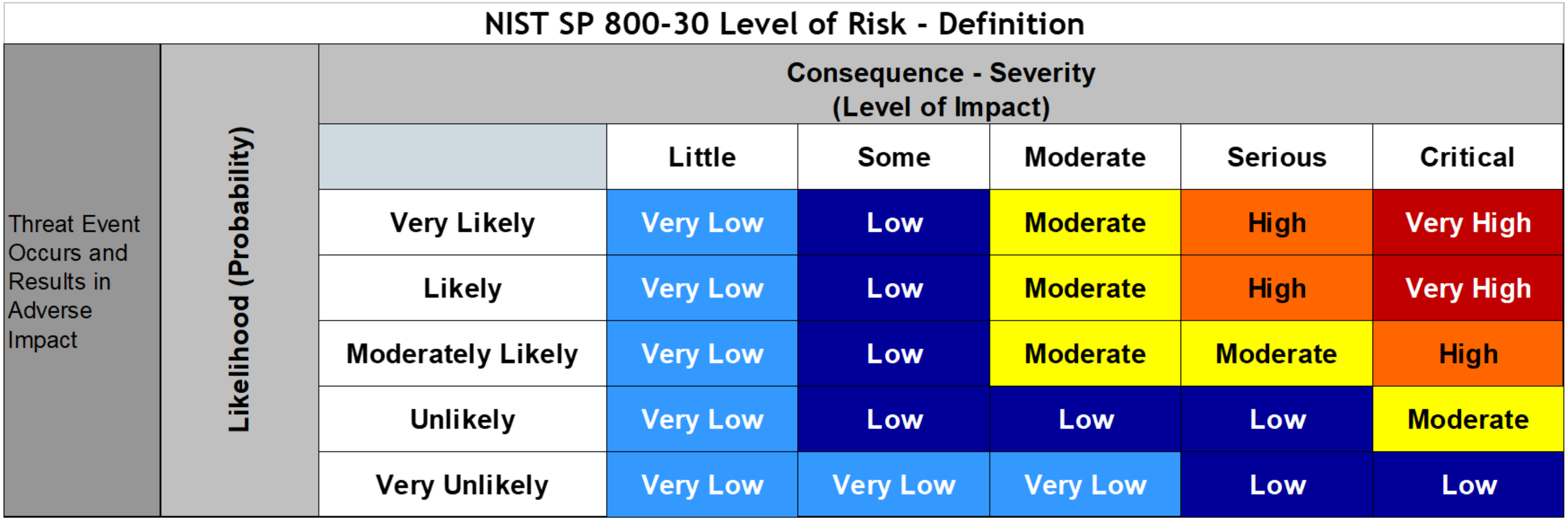
- Clean desk review of key areas at:
  - Public Services Building
  - Archives
- Data Center Review
- Telecom Demarcation Room review

Scope – Social Engineering

- Onsite
  - Attempts to piggyback into secured areas
- Email Phishing
  - Send specially crafted email messages to sample of staff
- Phone Calls
  - Calls to random sample of staff with purpose of getting access to systems and data

Scope - Risk Assessment

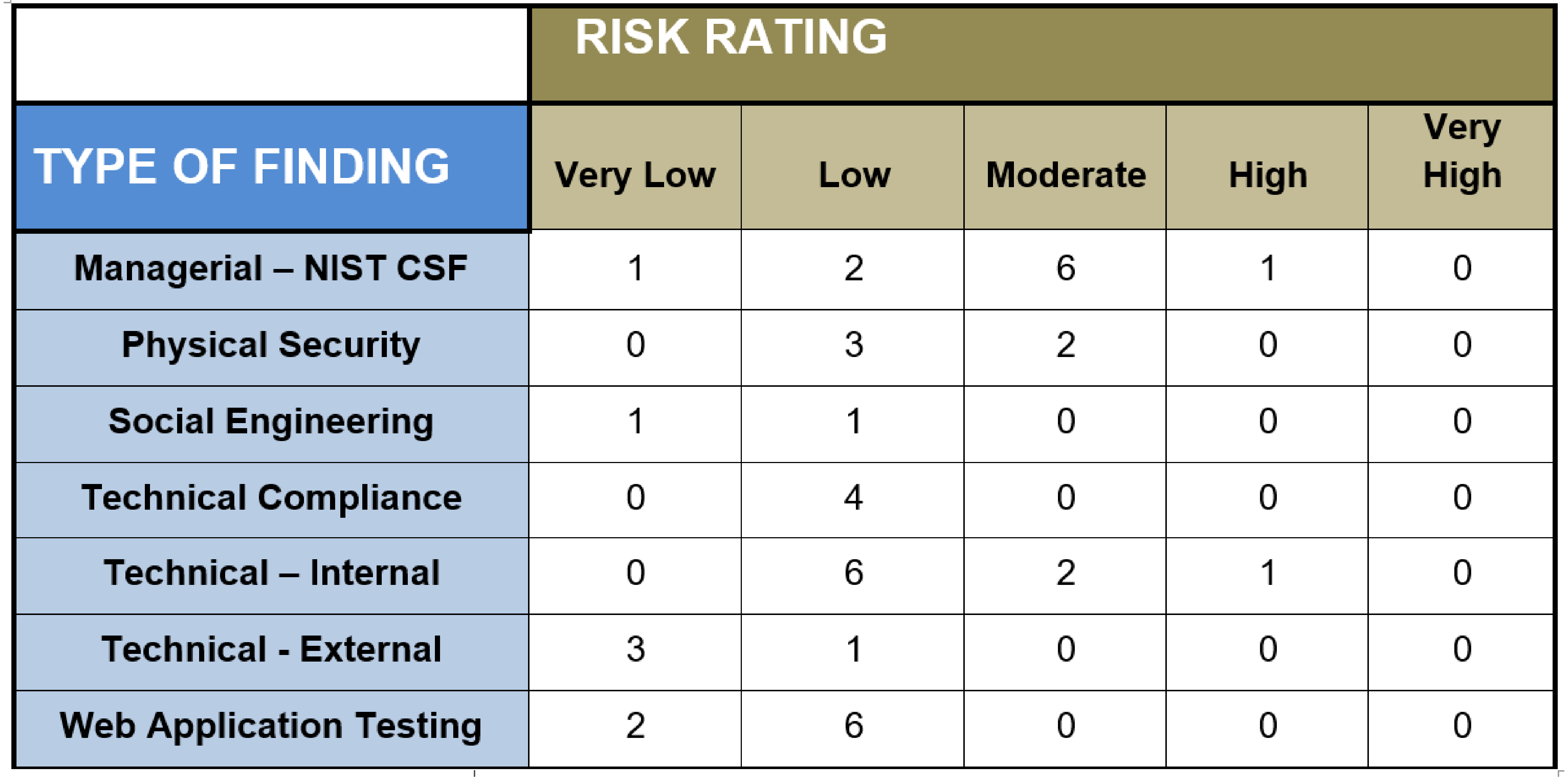
- Assessment of risk for the organization based upon observed controls



NIST SP 800-30 Level of Risk - Definition

			Consequence - Severity (Level of Impact)				
			Little	Some	Moderate	Serious	Critical
Threat Event Occurs and Results in Adverse Impact	Likelihood (Probability)	Very Likely	Very Low	Low	Moderate	High	Very High
		Likely	Very Low	Low	Moderate	High	Very High
		Moderately Likely	Very Low	Low	Moderate	Moderate	High
		Unlikely	Very Low	Low	Low	Low	Moderate
		Very Unlikely	Very Low	Very Low	Very Low	Low	Low

Risk Assessment Summary



	RISK RATING				
TYPE OF FINDING	Very Low	Low	Moderate	High	Very High
Managerial – NIST CSF	1	2	6	1	0
Physical Security	0	3	2	0	0
Social Engineering	1	1	0	0	0
Technical Compliance	0	4	0	0	0
Technical – Internal	0	6	2	1	0
Technical - External	3	1	0	0	0
Web Application Testing	2	6	0	0	0

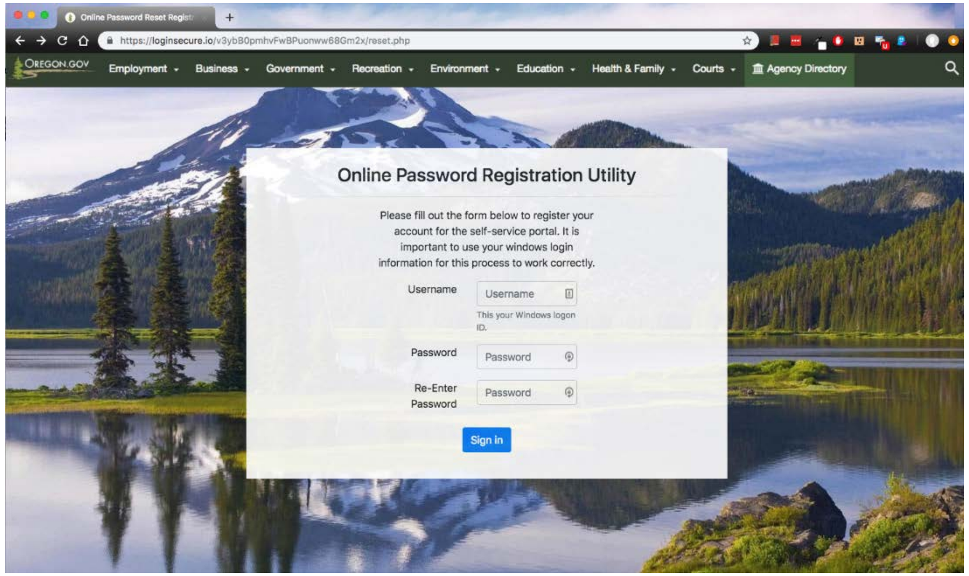
Physical Security - Summary

- Over all controls are good and meet NIST CSF recommendations
- No sensitive CJIS or PII data was found unsecured
- Primary concern is unsecured written credentials
- Datacenter has many best practices but a few low risk concerns exist

Social Engineering Summary

Low Risk

- Attempted Tailgating against multiple doors and targets
    - Stopped all times
    - Staff are well trained and polite – Asked to help and directed
- Phone Calls – Vishing
    - Cerium called 26 staff and spoke to ten
    - Nine of the ten responded appropriately
    - One staff member ran commands an attempted to connect to an external website
    - Technical controls prevented exploits from working
- Email Phishing
    - Technical controls prevented spoofing
    - 102 emails sent
    - Nine site clicks
    - Seven form submissions
    - IT Staff shut down access within 35 minutes



https://loginsecure.io/v3ybB0pmhvFwBPuonww68Gm2x/reset.php

Online Password Registration Utility

Please fill out the form below to register your account for the self-service portal. It is important to use your windows login information for this process to work correctly.

Username: Username

This your Windows logon ID.

Password: Password

Re-Enter Password: Password

External Penetration Testing Summary

Low Risk

- Technical Mitigations and Monitoring are Excellent
  - Received no results initially after scanning IP was blocked
  - Required whitelisting of scanning IP
- Results
  - Few low risk patching issues
  - Some cleartext legacy protocols are enabled

WAPT Summary

- Penetration testing based on OWASP Testing Framework v4
- Some vulnerabilities were identified but all low to informational.
- Of the vulnerabilities identified most are mitigated by WAF or other controls.
- Cerium found the organization’s monitoring and intrusion prevention controls to be very strong.

Summary - Internal Technical Findings

- Patch management is excellent
  - Only a few minor patches missing – Low risk
- Configuration management is good with some issues
  - Few Open shares – Medium risk
  - No authentication required for one application – Medium risk
  - Minor issue with Windows configuration – V. Low risk
- There are several issues with legacy software and services
  - Older Windows OS – High risk
  - Older data bases and web server – Medium risk
  - Several legacy services that disclose info or are cleartext - Low risk

Oracle Databases CIS Security Review

- Mostly compliant with CIS Standard
- Few low risk issues
- Recommendations
  - Improved auditing
  - Improved encryption
  - Improved access controls

CheckPoint Firewall Configuration Review

- Mostly compliant with Best Practice Review
- Few low risk issues
- Recommendations
  - Improved authentication
  - Improved access control parameters
  - Improvement on outbound rules

VMWare CIS Security Review

- Mostly non-compliant with CIS Standard
- Low Risk Issue
- Recommendations
  - Turn off features that are not needed or used
  - Improved logging
  - Improved console configuration

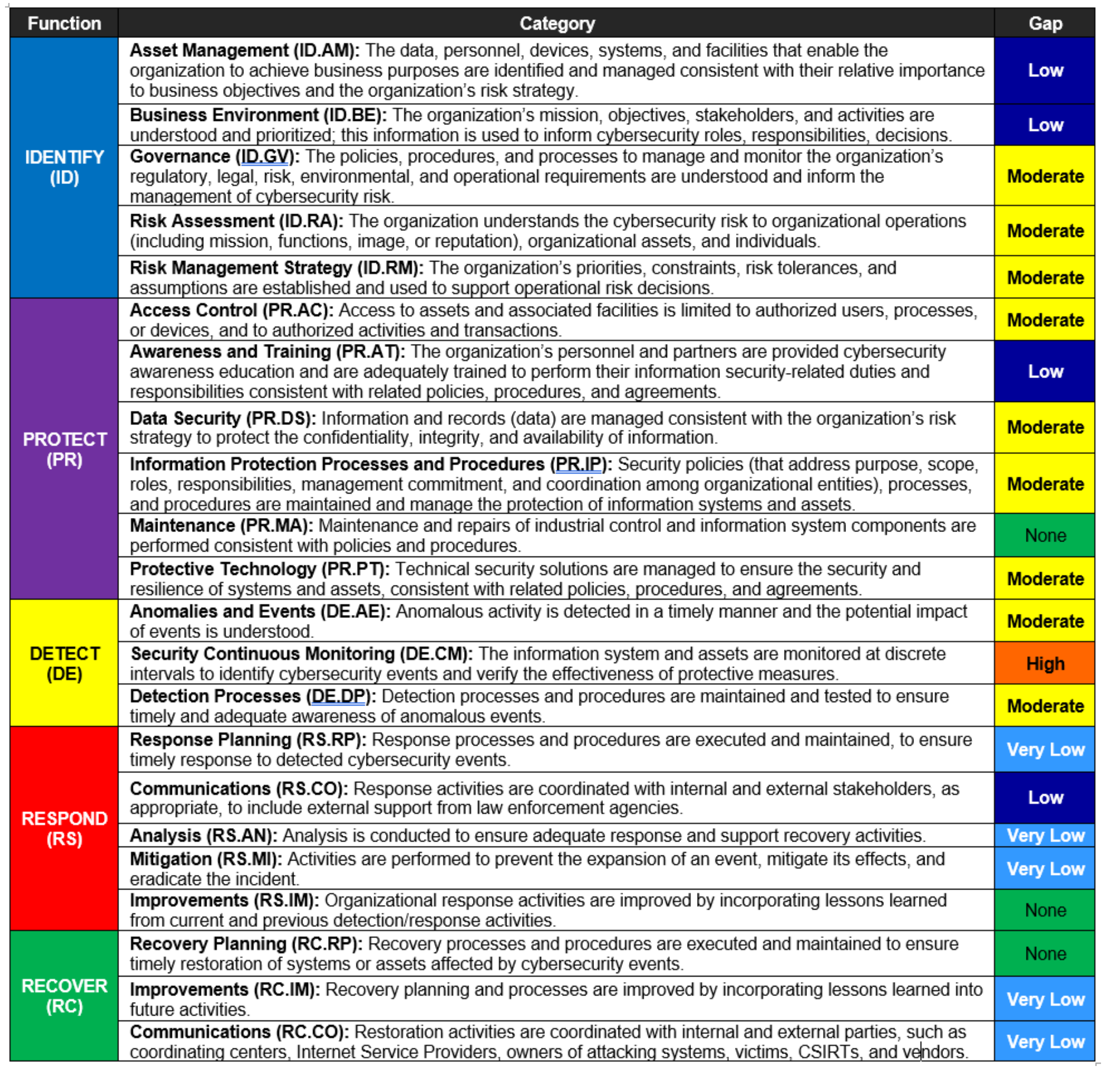
Cisco Switches CIS Security Review

- Mostly Non-Compliance with CIS Standard
- Low Risk Issue
- Recommendations
  - Improved crypto settings
  - Improved authentication
  - Remove legacy settings

Managerial Findings Summary

- Process and document review based on NIST Cyber Security Framework which is based on NIST 800-53 and FISMA Requirements
- Gaps exist but only one HIGH Risk Gap
- This shows that the organization has many good controls but that written documentation is lacking and budget constraints and resources have prevented improvements in many areas
- Along with recognizing deficiencies in controls, the assessment also provides an opportunity for information sharing and discovery while establishing a baseline security profile

NIST-CSF Heat Map



Function	Category	Gap
IDENTIFY (ID)	**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 business objectives and the organization's risk strategy.	Low
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, decisions.	Low
	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.	Moderate
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Moderate
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Moderate
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	Moderate
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	Low
	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.	Moderate
	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 manage the protection of information systems and assets.	Moderate
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	None
	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.	Moderate
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	Moderate
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	High
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	Moderate
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	Very Low
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	Low
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	Very Low
	Mitigation (RS.MI): Activities are performed to prevent the expansion of an event, mitigate its effects, and eradicate the incident.	Very Low
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	None
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	None
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Very Low
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, CSIRTs, and vendors.	Very Low

NIST CSF Recommendations

- Improved documentation
  - Many processes are not formalized
  - Policies are lacking in some areas
- Improvements on some technical controls
- Improved access control settings
- Improvements to detection and protection processes
- Improvements to media, device, and data protections