RISK MANAGEMENT PLAN AND IMPLEMENTATION GUIDE FOR HGA AND HIC

Class Project Paper

DECEMBER 10, 2020

BY ALEXANDER SEMAAN
CY 5200 – Fall 2020

Table of Contents

PART A - Security Risk Management Assessment

I. Executive Summary

1. Information System Name/Title

This report is being completed for Hypothetical Government Agency – HGA.

2. Information Asset Categorization

Asset	Impact		
	Confidentiality	**Integrity**	**Availability**
Financial Resources	High	High	High
System Components	High	High	High
Personnel Information	High	High	Medium
Contracting and Procurement Document	High	High	High
Draft Regulation	High	High	Medium
Internal Correspondence	High	High	High
Business Documents, Memos and Reports	High	High	High

HGA's Information System is categorized as High.

3. Information System Owner

Name: Giannis Anteto
Title: Chief Information Officer (CIO)
Agency: Hypothetical Government Agency (HGA)
Address: 10 Commonwealth Avenue, Boston, MA, 02116
Email: Anteto.G@hga.gov
Phone Number: (617)202-1337

4. Authorizing Official

Name: Lebron Dagger
Title: Chief Executive Officer (CEO)
Agency: Hypothetical Government Agency (HGA)
Address: 269 Commonwealth Avenue, Boston, MA, 02116
Email: Dagger.L@hga.gov
Phone Number: (617)202-5208

5. Other Designed Contacts

Name: Anthony Brows
Title: Chief Technology Officer (CTO)
Agency: Hypothetical Government Agency (HGA)

Address: 411 Marlborough Street, Boston, MA, 02115
Email: Brows.A@hga.gov
Phone Number: (617)202-9549

6. Assignment of Security Responsibility

Name: Hairy Potter
Title: Chief Information Security Officer (CISO)
Agency: Hypothetical Government Agency (HGA)
Address: 416 Marlborough Street, Boston, MA, 02115
Email: Potter.H@hga.gov
Phone Number: (617)202-2020

7. Information System Operational Status

HGA's Information Systems are operational.

8. Information System Type

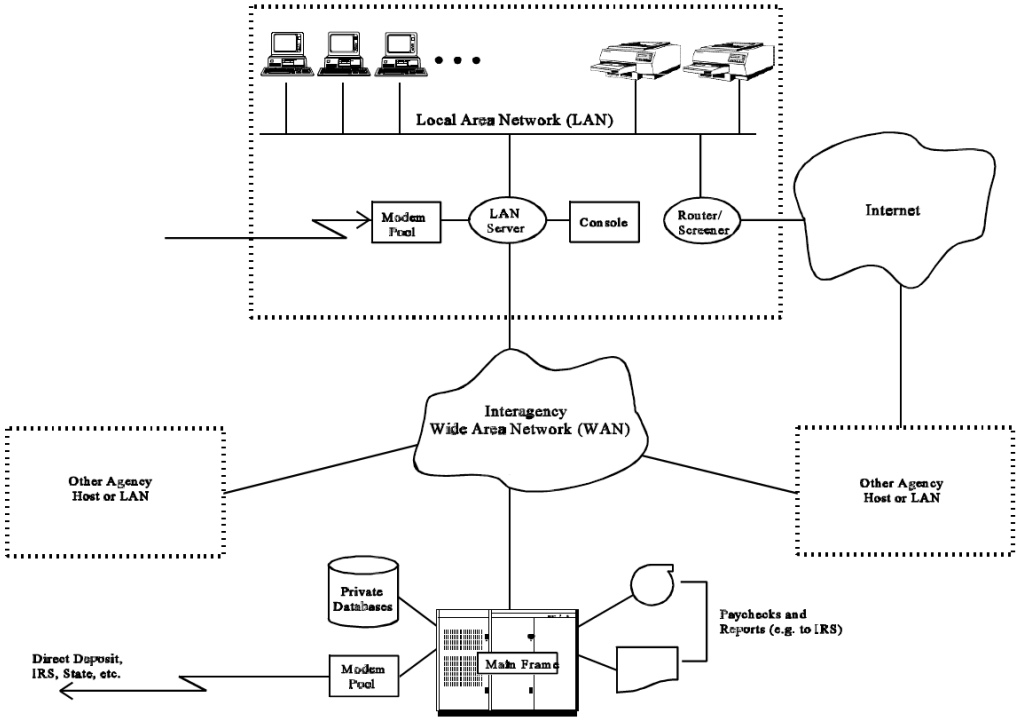
HGA's Information System Type relates to several major applications.

9. General System Description/Purpose

HGA's main mission is to handle Payrolls and to transfer US Government funds to individuals through the use of paychecks. This makes HGA's financial resources their greatest asset.

10. System Environment

HGA has a straightforward system topology and infrastructure that is portrayed in the image below. Most devices such as PCs and printers are connected to a LAN server. The LAN server is also responsible for connecting modem pools as well as special consoles that employees use to log-in to HGA's system. The main security control mechanism that the LAN server deploys is an Access Control infrastructure, and the access is given after written consent. For internet access, HGA has a main internet-facing router and for HGA to connect with other agencies, as well as a mainframe, their LAN server is connected to a WAN that offers all of the above.



11. System Interconnections / Information Sharing

System Name: Government Agency Hypo Network
Organization Type: Telecommunications Company
System Type: General Support System
Agreement: Government Contract
Date: Nov 5, 1996
FIPS 199 Category: High
C&A Status: NIST certified and Accredited
Authorization Official: Carmela Soprano

12. Related Laws/Regulations/Policies

Payment Card Industry Data Security Standard (PCI DSS)
NIST Risk Management Framework (NIST 800 guidelines)
Gramm-Leach-Bliley Act (GLBA)
Privacy Act of 1974
Federal Information Processing Standard – 199 (FIPS – 199)

13. Minimum Security Controls

A table describing the 17 MOT controls and their implementation for HGA.

Control	Implementation	Status	Control Type	Authority Responsible

Risk Management (M1)	Completion of risk assessment and provide recommendations	Implemented	Common Control	CISO
Life Cycle Support (M2)	Life cycle for the system's development is well prepared	Partially implemented	Common Control	CIO
Authorization Process (M3)	System needs to receive accreditation and certification periodically	Not implemented	Common Control	CISO
Management Planning (M4)	Implement a security plan for systems and provide a privacy impact assessment	Partially Implemented	Common Control	CISO
Personnel Security (O1)	Cover all personnel security policies and procedures	Implemented	Common Control	CISO
Physical and Environmental Protection (O2)	Making sure physical access control is in place and security cameras, cable management as well as emergency shutoff	Partially Implemented	Common Control	CIO
Contingency Planning (O3)	Prepare policies and procedures, train staff, plan tests and exercises. Having alternate storage site and backups.	Implemented	Common Control	CIO
Configuration Management (O4)	Prepare policies and procedures for configuring new systems, such as security impact analysis and system inventorying.	Partially Implemented	Common Control	CISO
Maintenance (O5)	Apply controlled maintenance in a timely manner, using specific maintenance tools	Partially Implemented	Common Control	CIO
System and Information Integrity (O6)	Create policies that ensure data integrity, timely patch deployment, network and endpoint monitoring with anti-virus, IPS…	Partially Implemented	Common Control	CISO
Security, Awareness, Training and Education (O7)	Train and educate personnel on security policies.	Implemented	Common Control	CISO
Incident Response Capability (O8)	Train personnel with tests and exercises for incident handling, monitoring, reporting and assisting	Partially Implemented	Common Control	CIO
Media Protection (O9)	Create policies for handling digital and non-digital media storage devices	Implemented	Common Control	CISO

Identification and Authentication (T1)	Manage user and device identification and authentication, and comply with encryption standards (such as FIPS')	Partially Implemented	Common Control	CISO
Access Control (T2)	Create policies for account management, access restrictions and use least privilege.	Partially Implemented	Common Control	CISO
Audit and Accountability (T3)	Place policies to perform timely audit reviews, analysis and reporting.	Not Implemented	Common Control	CISO
System and Communications Protection (T4)	Create policies to ensure partitioning database for different apps, protect against DoS attacks, transmit over encrypted and safe data links with the use of firewalls and boundary monitoring	Not Implemented	Common Control	CISO

14. Information System Security Plan Completion Date

10.10.2020

15. Information System Security Plan Approval Date

10.11.2020

II. List of Assets

S.No.	Asset Type	Value
A1	Financial Resources	$5,000,000
A2	System Components	
A21	PCs	$450,000
A22	LAN Server	$100,000
A23	Printers	$18,000
A24	Routers	$60,000
A25	Modem Pools	$6,000
A26	Special Consoles	$18,000
A3	Personnel Information	$400,000
A4	Contracting and Procurement Document	$45,000
A5	Draft Regulation	$55,000

A6	Internal Correspondence	$10,000
A7	Business Documents, Memos and Reports	$500,000
A8	Reputation	Intangible
A9	Employee Confidence	Intangible

Subset of Assets

S.No.	Asset Type	Value
A1	Financial Resources	$5,000,000
A21	PCs	$450,000
A24	Routers	$60,000
A3	Personnel Information	$400,000

III. List of Threats

S.No.	Threats
T1	Payroll Fraud
T2	Payroll Errors
T3	Interruption of Operations
T4	Disclosure or Brokerage of Information
T5	Network-Related Attacks
T6	Other Threats

Subset of Threats

S.No.	Threats
T1	Payroll Fraud
T3	Interruption of Operations
T4	Disclosure or Brokerage of Information
T5	Network-Related Attacks

IV. List of Vulnerabilities

S.No.	Vulnerability
T1V1	Vulnerabilities Related to Payroll Fraud
T1V11	Falsified Time Sheets
T1V12	Unauthorized Access
T1V13	Bogus Time and Attendance Applications
T1V14	Unauthorized Modifications of Time and Attendance Sheets
T2V2	Vulnerabilities Related to Payroll Errors
T3V3	Vulnerabilities Related to Continuity of Operations
T3V31	COG Contingency Planning
T3V32	Division Contingency Planning
T3V33	Virus Prevention
T3V34	Accidental Corruption and Loss of Data
T4V4	Vulnerabilities Related to Information Disclosure or Brokerage
T5V5	Network-Related Vulnerabilities
T6V6	Other Vulnerabilities

Subset of Vulnerabilities

S.No.	Vulnerability
T1V12	Unauthorized Access
T3V34	Accidental Corruption and Loss of Data
T4V4	Vulnerabilities Related to Information Disclosure or Brokerage
T5V5	Network-Related Vulnerabilities

V. Threat/Vulnerabilities Pairs

Vulnerability	Threat

	T1	**T3**	**T4**	**T5**
T1V12 on A1,A21,A24,A3	75	75	85	40
T3V34 on A1,A21,A24,A3	10	80	10	10
T4V4 on A1,A21,A24,A3	10	10	80	10
T5V5 on A1,A21,A24,A3	25	75	25	90

VI. Assets impacted by Threat/Vulnerability Pairs

Assets	**Vulnerabilities**
A1 Financial Resources	T1V12: Unauthorized Access
	T3V4: Accidental Corruption and Loss of Data
	T4V4: Vulnerabilities Related to Information Disclosure or Brokerage
	T5V5: Network Related Vulnerabilities
A21 PCs	T1V12: Unauthorized Access
	T3V4: Accidental Corruption and Loss of Data
	T4V4: Vulnerabilities Related to Information Disclosure or Brokerage
	T5V5: Network Related Vulnerabilities
A24 Routers	T1V12: Unauthorized Access
	T3V4: Accidental Corruption and Loss of Data
	T4V4: Vulnerabilities Related to Information Disclosure or Brokerage
	T5V5: Network Related Vulnerabilities
A3 Personnel Information	T1V12: Unauthorized Access
	T3V4: Accidental Corruption and Loss of Data
	T4V4: Vulnerabilities Related to Information Disclosure or Brokerage
	T5V5: Network Related Vulnerabilities

VII. MOT – which MOT controls are covered by current HGA controls (Histogram)

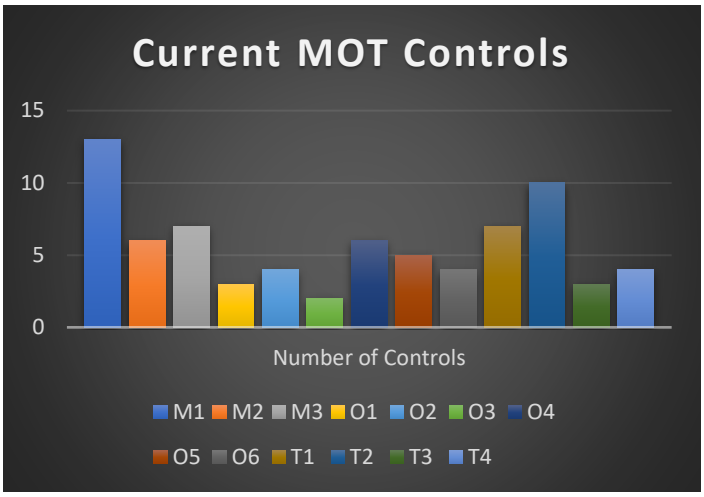
Current and Proposed M-O-T Controls

Management	Operational	Technical
Risk Management (M1)	Personnel/User Issues (O1)	Identification and Authentication (T1)
Program Management (M2)	Contingencies and Disaster Planning (O2)	Logical Access Control (T2)
Policies (M3)	Incident Reporting and Handling (O3)	Audit Trails (T3)
	Awareness, Training and Education (O4)	Cryptography (T4)
	Security Considerations in Support and Operations (O5)	
	Physical and Environmental Security (O6)	

Current Security Controls and Policies

S.No.	Security Controls and Policies	M-O-T Controls	Common Criteria
C1	General Use and Administration of HGA's Computer System		
C11	Login IDs and Passwords	M1-O1-O4-T1-T4	RA1-RA2-PS1-CP1-AT1-IA1-SC13
C12	Written Authorization from Supervisors	M2-M3-O1-O5-T1-T2-T3	PL1-CA6-PS1-CP1-SI1-IA1-AC1-AU1
C13	Security Awareness and Training Course	M2-M3-O4	PL1-CA6-AT1-
C14	Automated Access Control Mechanism	M1-O1-O5-T2	RA1-PS1-SI1-AC1-
C2	Time and Attendance Application		
C21	Protection Against Unauthorized Access	M1-T1-T2-T4	RA1-IA1-AC1-SC13
C22	Protection Against Payroll Errors	M1-O4	RA1-AT1

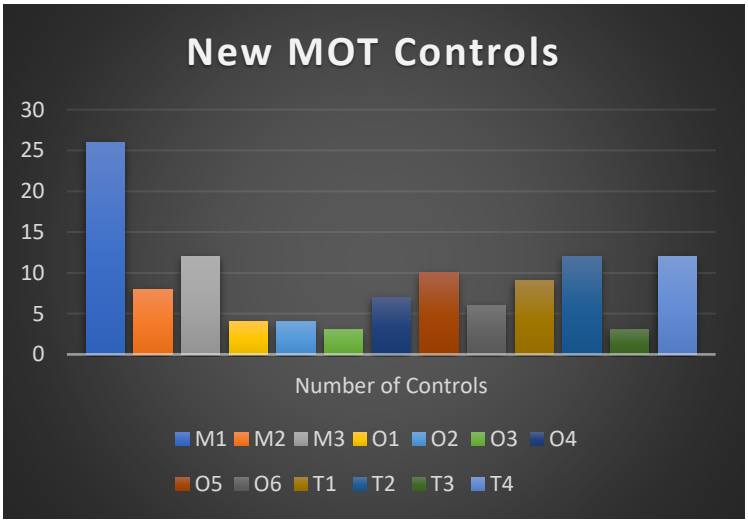
C23	Protection Against Accidental Corruption or Loss of Payroll Data	M1-O2-O5-T4	RA1-PE1-SI1-SC13
C3	Protection Against Interruption of Operations		
C31	COG Contingency Planning	M2-O2-O6	PL1-PE10-
C32	Reviewing Audit Logs	M1-M3-O5-T3	RA1-CA6-SI1-AU1
C33	Report indications of security violations in audits to Incident Handling Team	M2-O3-T3	PL1-CP1-
C34	Division Contingency Planning	M2-O2-O6	PL1-PE10-
C4	Protection Against Disclosure or Brokerage of Information		
C41	Secure Storage of Time and Attendance Paper Documents and disclosure-sensitive information stored on floppy disks and other removable magnetic media	M1-M3-O4-O5-O6-T2	RA1-CA6-SI1-AT1-AC1
C42	PC-disabling key lock	M1-O4-O6-T1-T2	RA1-AT1-IA1-AC1
C43	Group-Oriented LAN Access Control	M1-T1-T2	RA1-IA1-AC1
C44	Security Awareness Training	M2-M3-O4	PL1-CA6-AT1-
C5	Protection Against Network-Related Threat		
C51	Limited External Network Interactions (Only Email and Data Transfers)	M1-M3-T1-T2	RA1-CA6-IA1-AC1
C52	Disallow All Remote Log-in Sessions to the Internet-facing Router	M1-T1-T2	RA1-IA1-AC1
C53	Special Access-Control Privilege Setup by System Administrators Only.	M1-M3-T2	RA1-CA6-AC1
C54	COG reports attacks to Incident Handling Team	O3	CP1-
C6	Protection Against Risks from Non-HGA Computer Systems	M1-O2-T2-T4	RA1-PE1-AC1-SC13



VIII. MOT – which MOT controls after improvements made by CISO recommendations, with new VPN server and DMZ (Histogram)

S.No.	New Controls	M-O-T Controls	Common Criteria
NC1	Controls Mitigating Vulnerabilities Related to Payroll Fraud		
NC11	Server Administrative Procedures and Bugfixes	M1-O5	RA2-RA5-SI1
NC12	One-Time Passwords	M1-M3-T4	RA1-CA6-SC13
NC13	Digital Signatures	M1-M3-O5-T1-T4	RA1-CA6-SI1-IA1-SC13
NC2	Controls Mitigating Payroll Error	M1-O1	RA1-RA2-PS1
NC3	Controls Mitigating Vulnerabilities Related to Continuity of Operations		
NC31	SETA	M1-M2-M3-O4	RA1-PL1-CA6-AT1
NC32	Mainframe MOU	M1	RA2
NC33	Automated E-mail Reminders	M2-O5-	PL1-SI1
NC4	Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of Information		
NC41	Screen Locks	M1-M3-O4-O6	RA1-CA6-AT1

NC42	Hard Disk Encryption	M1-M3-O2-T4	RA1-PE1- SC13
NC5	Controls Vulnerabilities Related to Network-Related Attacks		
NC51	Stronger I&A	M1-O5-T4	RA1-SI1-SC13
NC52	Encrypting Modems	M1-T4	RA1-SC13
NC53	Mainframe Communications Encryption	M1-T4	RA1-SC13
NC6	VPN Server	M1-M3-O6-T1-T2-T4	RA1-CA6-IA1-AC1-SC13
NC7	DMZ	M1-M2-O3-O5-T2-T4	RA1-PL1-CP1-SI1-AC1-SC13



IX. Security Risk Prevention Strategy

Phase 0 – Current, recommended, missing, VPN and DMZ Controls Comparison to the 157 risk controls from Common Criteria.

The comparison for current, recommended, VPN and DMZ Controls is included in sections VII and VIII. The comparison to missing controls will be included while describing the missing/new controls.
The Common Criteria Controls that are completely missing include some of the following: Security planning, life cycle support, system and applications assurance, Developer Security Testing, Continuous Monitoring, thorough Personnel Screening and Security, configuration management, maintenance, audit trails and accountability, as well as the use of PKI and IDS/IPS software.

Phase 1 – Initial Improvements and added controls

Replacing the modem pool with a VPN server reduces probability of exploitation on vulnerabilities for all threats. In fact, VPN allows for a more secure remote access connection that employees can use more confidently. VPN provides confidentiality and integrity, as the traffic is tunneled, meaning that it is encrypted and travels the internet securely. This minimizes risk related to information disclosure or brokerage, and it also helps with controlling unauthorized access, all while reducing likelihood of network-related attacks that were possible on the previous modem pools. Adding a screened subnet with DMZ enforces security controls, and certainly helps with access control and organizing the network architecture, while limiting damage in case of an intrusion.

The VPN server's asset value can be estimated at about $6,000 dollars (6 servers for $1,000 each). The firewalls needed to setup and protect the DMZ would cost about $30,000 (6 cisco firewalls for $5,000 each).

Updated Assets Inventory

S.No.	Asset Type	Value
A1	Financial Resources	$5,000,000
A2	System Components	
A21	PCs	$450,000
A22	LAN Server	$100,000
A23	Printers	$18,000
A24	Routers	$60,000
A25	VPN servers	$6,000
A26	Special Consoles	$18,000
A27	DMZ Firewalls	$30,000
A3	Personnel Information	$400,000
A4	Contracting and Procurement Document	$45,000
A5	Draft Regulation	$55,000
A6	Internal Correspondence	$10,000
A7	Business Documents, Memos and Reports	$500,000
A8	Reputation	Intangible
A9	Employee Confidence	Intangible

Missing MOT Controls

List of Missing M-O-T Controls		
Management	**Operational**	**Technical**
Life Cycle Planning	(all have been addressed)	Audit Trails
Assurance		

Subset of Critical Assets Selected

S.No.	Asset Type	Value
A1	Financial Resources	$5,000,000
A21	PCs	$450,000
A24	Routers	$60,000
A25	VPN Servers	$6,000
A27	DMZ Firewalls	$30,000
A3	Personnel Information	$400,000
A7	Business Documents, Memos and Reports	$500,000

With these two new assets come certain liabilities: although VPN is a great improvement over Modem pools, it does create a new threat vector and a new set of vulnerabilities related to VPNs has to be considered. In fact, there are certain flaws with VPN that have been discovered, and we will assume that they have not been patched by HGA. There are some Remote Code Execution (RCE) vulnerabilities that have been disclosed (like the Palo Alto GlobalProtect Portal vuln CVE-2019-1579), as well as these vulnerabilities: CVE-2019-11510, CVE-2019-11539, CVE-2018-13379 and more.

This creates **T7 (VPN-related attacks)** and **V7 (VPN-related vulnerabilities).**

Threat/Vulnerability Matrix with probability of exploitation

Vulnerability	Threat				
	T1	**T3**	**T4**	**T5**	**T7**
T1V12 on A1,A21,A24,A25,A27,A3,A7	40	50	50	25	60
T3V34 on A1,A21,A24,A25,A27,A3,A7	15	60	15	15	15
T4V4 on A1,A21,A24,A25,A27,A3,A7	15	15	70	15	70

T5V5 on A1,A21,A24,A25,A27,A3,A7	20	50	20	65	75
T7V7 on A1,A21,A24,A25,A27,A3,A7	15	15	30	65	80

Risk Impact

Again, we will show no flexibility for asset resilience, hence the risk impact is High, meaning that once a threat exploits a vulnerability, we assume total asset loss, for both Phase 1 and Phase 2.

Assets	Threat exploits a vulnerability																								
	T1V12	T1V34	T1V4	T1V5	T1V7	T3V12	T3V34	T3V4	T3V5	T3V7	T4V12	T4V34	T4V4	T4V5	T4V7	T5V12	T5V34	T5V4	T5V5	T5V7	T7V12	T7V34	T7V4	T7V5	T7V7
A1	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A21	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A24	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A25	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A27	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A3	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A7	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100

Residual Asset Security Risk (See Appendix A1 for calculations)

Risk of A1= 5000000 (total loss of asset).
Risk of A21 = 450000 (total loss of asset).
Risk of A24 = 60000 (total loss of asset).
Risk of A25 = 6000 (total loss of asset).
Risk of A27 = 30000 (total loss of asset).
Risk of A3 = 400000 (total loss of asset).
Risk of A7 = 500000 (total loss of asset).

Residual Risk of all Assets = 6446000

Ranking of security asset residual risks

Rank	Asset
1	A1: Financial Resources
2	A7: Business Documents, Memos and Reports
3	A21: PCs
4	A3: Personnel Information
5	A24: Routers
6	A27: DMZ Firewalls
7	A25: VPN Servers

Vulnerability Security Risk (See Appendix A2 for calculations)

Risk due to T1V12 = $14,503,500
Risk due to T3V34 = $7,735,200
Risk due to T4V4 = $11,925,100
Risk due to T5V5 = $14,825,800
Risk due to T7V7 = $15,214,300

Ranking of vulnerability security risks

Rank	Vulnerability
1	T5V5: Network-Related Vulnerabilities
2	T1V12: Unauthorized Access
3	T7V7: VPN related Vulnerabilities
4	T4V4: Vulnerabilities Related to Information Disclosure or Brokerage
5	T3V34: Accidental Corruption or Loss of Data

Phase 2 – Additional Risk Prevention Controls

To bring down the likelihood of successful attacks on HGA's network, I would recommend third party Denial of Service Mitigation services, such as Cloudfare can prove very useful against DoS attacks (Common Criteria – SC5), helping reduce mostly interruption of operations. Also, patching network vulnerabilities, VPN vulnerabilities and keeping a strong posture around patching and vulnerability management processes will significantly reduce likelihood of successful attacks (Common Criteria - RA5).

Additionally, previous controls proposed by new CISO did not include best security practices when it comes to login authentication. It is imperative that HGA configures Multi-Factor Authentication for its users by the use of OTP or RSA keys as well as a biometric option (fingerprint or face-id using webcams) so there could be no mistake and to minimize the risk associated to unauthorized access (Common Criteria – IA7).

Threat/Vulnerability Matrix with probability of exploitation

Vulnerability	**Threat**				
	T1	**T3**	**T4**	**T5**	**T7**
T1V12 on A1,A21,A24,A25,A27,A3,A7	10	15	15	10	15
T3V34 on A1,A21,A24,A25,A27,A3,A7	15	30	15	15	15
T4V4 on A1,A21,A24,A25,A27,A3,A7	15	15	20	15	10
T5V5 on A1,A21,A24,A25,A27,A3,A7	5	10	5	25	15
T7V7 on A1,A21,A24,A25,A27,A3,A7	10	15	15	20	25

Residual Asset Security Risk (See Appendix A3 for calculations)

Risk of A1= 5000000 (total loss of asset).
Risk of A21 = 450000 (total loss of asset).
Risk of A24= 60000 (total loss of asset).
Risk of A25= 6000 (total loss of asset).
Risk of A27= 30000 (total loss of asset).
Risk of A3= 400000 (total loss of asset).
Risk of A7= 500000 (total loss of asset).

Residual Risk of all Assets = 6446000

Ranking of security asset residual risks

Rank	**Asset**
1	A1: Financial Resources
2	A7: Business Documents, Memos and Reports
3	A21: PCs
4	A3: Personnel Information
5	A24: Routers
6	A27: DMZ Firewalls
7	A25: VPN Servers

Vulnerability Security Risk (See Appendix A4 for calculations)

Risk due to T1V12 = $4,189,900
Risk due to T3V34 = $5,801,400
Risk due to T4V4 = $4,834,500
Risk due to T5V5 = $3,867,600
Risk due to T7V7 = $5,479,100

Ranking of vulnerability security risks

Rank	**Vulnerability**
1	T3V34: Accidental Corruption or Loss of Data
2	T7V7: VPN related Vulnerabilities
3	T4V4: Vulnerabilities Related to Information Disclosure or Brokerage

4	T1V12: Unauthorized Access
5	T5V5: Network-Related Vulnerabilities

X. Security Risk Response Strategy

As seen in Phase 1 and 2 of the Security Risk Prevention Strategy, Financial Resources are the assets with most residual risk, and the best way to deal with that is to restrict services and access to financial services. Additionally, all transactions related to HGAs financial resources (such as equity or bond sales, to employee salary distribution, and others) should go through an approval process by two people so that there is no single point of failure and this reduces risk immensely (Common Criteria – AC3, AC4)

Threat/Vulnerability Matrix with probability of exploitation

Vulnerability	**Threat**				
	T1	**T3**	**T4**	**T5**	**T7**
T1V12 on A1,A21,A24,A25,A27,A3,A7	10	15	15	10	15
T3V34 on A1,A21,A24,A25,A27,A3,A7	15	30	15	15	15
T4V4 on A1,A21,A24,A25,A27,A3,A7	15	15	20	15	10
T5V5 on A1,A21,A24,A25,A27,A3,A7	5	10	5	25	15
T7V7 on A1,A21,A24,A25,A27,A3,A7	10	15	15	20	25

Risk Impact

This time we will show more flexibility in regard to asset resilience, meaning that if a vulnerability is exploited the affected assets' value will not be 0 (completely destroyed).

Assets	**Threat exploits a vulnerability**																									
	T1V12	T1V34	T1V4	T1V5	T1V7	T3V12	T3V34	T3V4	T3V5	T3V7	T4V12	T4V34	T4V4	T4V5	T4V7	T5V12	T5V34	T5V4	T5V5	T5V7	T7V12	T7V34	T7V4	T7V5	T7V7
A1	3	3	3	3	5	5	3	3	3	3	5	3	3	3	3	5	3	3	3	3	3	3	3	3	3
A21	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A24	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A25	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A27	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A3	30	15	15	10	10	20	20	25	5	10	10	20	15	10	15	10	10	10	10	15	15	20	15	20	15
A7	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100

Residual Asset Security Risk (Appendix B for Calculations)

Risk of A1= $612,500 (partial loss of asset).
Risk of A21 = $450,000 (total loss of asset).
Risk of A24= $60,000 (total loss of asset).

Risk of A25= $6,000 (total loss of asset).
Risk of A27= $30,000 (total loss of asset).
Risk of A3= $227,000 (partial loss of asset).
Risk of A7= $500,000 (total loss of asset).

Residual Risk of all Assets = $1,725,500

Ranking of security asset residual risks

Rank	Asset
1	A1: Financial Resources
2	A7: Business Documents, Memos and Reports
3	A21: PCs
4	A3: Personnel Information
5	A24: Routers
6	A27: DMZ Firewalls
7	A25: VPN Servers

Vulnerability Security Risk (Appendix B for calculations)

Risk due to T1V12 = $860,400
Risk due to T3V34 = $1,139,400
Risk due to T4V4 = $945,000
Risk due to T5V5 = $745,600
Risk due to T7V7 = $1,072,600

Ranking of vulnerability security risks

Rank	Vulnerability
1	T3V34: Accidental Corruption or Loss of Data
2	T7V7: VPN related Vulnerabilities
3	T4V4: Vulnerabilities Related to Information Disclosure or Brokerage
4	T1V12: Unauthorized Access
5	T5V5: Network-Related Vulnerabilities

XI. Mixed Security Risk Strategy – Prevention and Response

The Mixed Security Risk Strategy can prove to be very effective as it allows for a combination of risk prevention and risk response controls to be implemented. In fact, it allows management to select the best of both worlds to structure an efficient strategy.

In this case, we will implement the controls from Phase 2 of the Risk Prevention Strategy as well as the controls from the Risk Response Strategy. Additionally, HGA should seek to strengthen their Incident Response plan facing physical and environmental accidents, as well as intrusions or breaches, by making quarterly revisions of their plan and policies, and implementing those that are missing (Common Criteria – IR1, CP1). This will reduce the risk impact on assets further, allowing for a stronger security posture.

Finally, the second most valuable asset is A7, Business Documents, Memos and Reports. We need to make sure that these documents are encrypted and stored securely with high-privilege access control and that the servers are located in the DMZ to further increase detection mechanisms (Common Criteria – AC1, AC6, SC13).

Threat/Vulnerability Matrix with probability of exploitation

Vulnerability	**Threat**				
	T1	**T3**	**T4**	**T5**	**T7**
T1V12 on A1,A21,A24,A25,A27,A3,A7	10	15	15	10	15
T3V34 on A1,A21,A24,A25,A27,A3,A7	15	30	15	15	15
T4V4 on A1,A21,A24,A25,A27,A3,A7	15	15	20	15	10
T5V5 on A1,A21,A24,A25,A27,A3,A7	5	10	5	25	15
T7V7 on A1,A21,A24,A25,A27,A3,A7	10	15	15	20	25

Risk Impact

This time we will show more flexibility in regard to asset resilience, meaning that if a vulnerability is exploited the affected assets' value will not be 0 (completely destroyed).

Assets	**Threat exploits a vulnerability**																									
	T1V12	T1V34	T1V4	T1V5	T1V7	T3V12	T3V34	T3V4	T3V5	T3V7	T4V12	T4V34	T4V4	T4V5	T4V7	T5V12	T5V34	T5V4	T5V5	T5V7	T7V12	T7V34	T7V4	T7V5	T7V7
A1	3	3	3	3	5	5	3	3	3	3	5	3	3	3	3	5	3	3	3	3	3	3	3	3	3
A21	10	15	15	10	15	20	15	10	15	20	30	15	5	10	15	15	10	15	15	10	15	20	15	10	10
A24	15	10	15	15	10	15	10	15	20	15	20	15	5	10	15	20	15	15	20	15	5	10	10	15	15
A25	5	5	5	15	20	5	5	10	15	20	10	10	10	15	25	10	10	10	15	20	10	15	15	20	50
A27	15	25	20	25	30	15	5	5	15	25	10	10	15	25	35	15	5	15	20	25	5	5	10	15	20
A3	30	15	15	10	10	20	20	25	5	10	10	20	15	10	15	10	10	10	10	15	15	20	15	20	15
A7	3	3	3	3	5	5	3	3	3	3	5	3	3	3	3	5	3	3	3	3	3	3	3	3	3

Residual Asset Security Risk (Appendix C for Calculations)

Risk of A1= $612,500 (partial loss of asset).
Risk of A21 = $237,375 (partial loss of asset).

Risk of A24= $30,600 (partial loss of asset).
Risk of A25= $3,360 (partial loss of asset).
Risk of A27= $18,150 (partial loss of asset).
Risk of A3= $227,000 (partial loss of asset).
Risk of A7= $61,250 (partial loss of asset).

Residual Risk of all Assets = $1,190,235

Ranking of security asset residual risks

Rank	Asset
1	A1: Financial Resources
2	A21: PCs
3	A3: Personnel Information
4	A7: Business Documents, Memos and Reports
5	A24: Routers
6	A27: DMZ Firewalls
7	A25: VPN Servers

Vulnerability Security Risk (Appendix C for calculations)

Risk due to T1V12 = $257,640
Risk due to T3V34 = $281,475
Risk due to T4V4 = $218,685
Risk due to T5V5 = $172,135
Risk due to T7V7 = $263,340

Ranking of vulnerability security risks

Rank	Vulnerability
1	T3V34: Accidental Corruption or Loss of Data
2	T7V7: VPN related Vulnerabilities
3	T1V12: Unauthorized Access
4	T4V4: Vulnerabilities Related to Information Disclosure or Brokerage
5	T5V5: Network-Related Vulnerabilities

XII. Different Strategy Budget Estimates

1. Risk Prevention Strategy (IX)

Total Budget Estimate for a Risk Prevention Strategy = $551,000 (See Appendix D1 for calculations)

2. Risk Response Strategy (X)

Total Budget Estimate for a Risk Response Strategy = $711,000 (See Appendix D2 for calculations)

3. Mixed Risk Strategy (XI)

Total Budget Estimate for a Mixed Risk Strategy = $771,000 (See Appendix D3 for calculations)

XIII. Conclusion – A Cost Benefit Analysis

HGA's risk management recommendations seem to be quite solid. Nevertheless, there is always room for improvement when it comes to cybersecurity. For instance, the recommendations for mitigating the identified vulnerabilities is on the money mostly, but in some areas the recommendations are outdated: authentication hardening should mention MFA, but they only mentioned OTPs.

Prior to the recommendations, HGA did a fair job at using the M-O-T model. The security policies they put in place seem to be fine, they also have great security considerations in support and operations. From a wholesome perspective, they addressed almost every point in the model, at the exception of Life Cycle Planning and Assurance. What is disappointing is that they have addressed the other M-O-T controls but very briefly and have not implemented the best security practices in each control.

HGA has issues with their audit program as it is not quite extensive, with compliance in regard to security policies being loosely followed, and their security program oversight is weak. Additionally, their Incident Response Team is not doing a good job handling quite a few incidents, so the management of this team should get a wake-up call.

Risk Prevention strategy aims to go after vulnerability prevention and it seems to do a great job at changing the ranking for vulnerability security risks, all while assuming no resilience when it comes to asset risk impact. On the other hand, Risk Response Strategy attempts to prioritize reducing assets' residual risk and reflects how an entity reacts to a security incident as opposed to proactively trying to prevent one. A mixed risk strategy utilizes both prevention and response security controls.

To visualize which strategy works best for HGA, we need to do a cost benefit analysis to see if controls for each strategy are worth implementing, and which strategy leads to the best cost-benefit ratio. First we need to see the improvement on residual risk (hence benefit from new controls for each strategy):

Strategy	Current Residual Risk	Residual Risk with New Controls	Residual Risk Reduction - Security Risk Benefit
Prevention	$6,446,000	$2,802,000	$3,644,000
Response	$6,446,000	$1,725,000	$4,721,000

Mixed	$6,446,000	$1,190,235	$5,255,765

Then we need to compute the Cost/Benefit Ratio:

Strategy	Residual Risk Reduction - Security Risk Benefit	New Controls Costs - Security Risk Budget Cost	Cost/Benefit Ratio
Prevention	$3,644,000	$551,000	0.151207464
Response	$4,721,000	$711,000	0.150603686
Mixed	$5,255,765	$761,000	0.144793384

According to the Cost/Benefit Ratio, HGA's best bet is on a Mixed strategy, as the benefits from reducing residual risk, all while taking into consideration the new controls implementation costs and budget, have proven to be superior to other strategies. One thing to keep in mind is that the budget and costs only include monetary value, and that it is important to consider Time as a resource as well, to see if HGA has time to implement all these new security controls. However, HGA doesn't have to implement everything all at once and can manage their time by looking closer at which security controls have the greatest risk reduction factors and start with those.

PART B – Security Risk Management Implementation Plan

The company I am doing this Risk Management Implementation Plan for requested that their name remains hidden for Legal disclosure purposes, so I will be calling it Hypothetical Investments Company (HIC). HIC is a financial and investments management firm, that also deals with asset management. Their security team is divided into two main categories: Security Engineers and Security Analysts, the heads of each team reports to the head of IT Production Control (also considered the CISO), who in turn reports to the CTO (also considered the CIO).

List of Company Critical Assets

S.No.	Asset Type	Value ($)
A1	Financial Resources	$100,000,000
A2	Client Investments	$70,000,000,000
A3	Client and Personnel Information	$50,000,000
A4	Network and Operations Systems	$10,000,000
A5	Business and IT Software/Apps	$3,000,000
A6	Client's Trust	Intangible

A7	Reputation	Intangible

List of Missing Controls, Vulnerabilities, Potential Threats, and Security Risks for:

1. Access Control Security Risk Management Implementation Controls and Policies

a. Identification Credentials
b. Personal Authentication
c. Authorization
d. Logical Access Control Methods
e. Physical Access Control Methods
f. Biometric Systems

Missing Controls

Missing or Partially Implemented Controls
Identification Credentials
Pin Code
PKI Certificate/Digital Signature
ID Card
Photograph
Biometric Authentication
Personal Authentication
Smart Card/Private Key/ Token
Biometric
Authorization
Smart Card/Security Token
Logical Access Control Methods
Network Architecture Controls
Encryption
PKI Compliance Requirements
Physical Tokens
Alternate Login Tokens
Physical Access Control Methods
Defense Biometric Identification System
Badges
Memory Cards
Smart Cards
Physical Tokens
Biometric Systems
Fingerprint Scanner
Facial Recognition System

Vulnerabilities

1. Unauthorized Access
2. Impersonation
3. Weak Authentication
4. Repudiation
5. Network-Related Vulnerabilities
6. Breach of Confidentiality and Integrity

Potential Threats

1. Disclosure of Confidential Information
2. Financial Theft
3. Intelligence and Information Gathering
4. Loss of Accountability and Trust
5. Network-Related Attacks

Risks

- Attackers can leverage repudiation and in the case of email communications, interception of messages is possible leading to a breach in confidentiality and to a loss of trust
- RFID card can be stolen or potentially duplicated to provide access to unauthorized individuals
- Does not match ID card to a face, leading to potential impersonation and to unauthorized access
- Identity theft not put in check, leading to potential impersonation and to unauthorized access
- Use of outdated network protocols can lead to successful network-related attacks, compromising integrity of the information systems as well as the confidentiality of data flowing across the network
- Weak LAN encryption for network services can reveal user credentials to potential packet sniffing on the LAN, giving attackers access to IT systems and apps
- Attackers can leverage repudiation and integrity verification weaknesses and in the case of email communications, interception of messages is possible leading to a breach in confidentiality and to a loss of trust
- Might lead to weak authentication, which can grant unauthorized access
- Identity theft not put in check, leading to potential impersonation and to unauthorized access of physical assets and resources.
- Weak authentication that can lead to potential impersonation and to unauthorized access of physical assets and resources.
- Identity theft not put in check, leading to potential impersonation and to unauthorized access of logical and physical assets and resources.

2. Network Infrastructure Security Risk Management Implementation Controls and Policies

a. Enclave Protection
b. Firewalls Risk Management
c. Routers Risk Management

Missing Controls

Missing or Partially Implemented Controls
Enclave Protection

Encryption
Network Test Access Ports (TAP)
Firewalls
Bastion Host
Stateful Inspection
Routers
Securing Router Planes

Vulnerabilities

1. Unauthorized Access
2. Credential Harvesting
3. Network Congestion
4. Poor IDS/IPS Performance
5. Weak Protection against Recon and Scanning Tools

Potential Threats

1. Network-Related Attacks
2. Compromised Network Node
3. Denial of Service
4. Malicious or Suspicious Traffic
5. Intelligence and Information Gathering

Risk

- Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view LDAP credentials in cleartext
- Lack of NTAP can lead to traffic congestion and delays due to IDS working in real-time and not on duplicate/mirrored packets, which can potentially lead to loss of services availability.
- Deep Inspection Firewalls are already configured and cover all of this firewall's capabilities
- Attackers can easily understand network topology and scan for vulnerable versions or Operating Systems using recon and scanning tools. Additionally they can perform DDoS attacks because ICMP echo requests are not disabled.

3. Network Infrastructure Management Security Risk Management Implementation Controls and Policies

a. Ports, Protocols, and Services (PPS) Risk Management
b. Device Risk Management
c. Device Monitoring, Network Management Risk Management
d. Network Authentication, Authorization, and Accounting Risk Management
e. Network Intrusion Detection Risk Management
f. Switches and VLANs Risk Management
g. Virtual Private Network Risk Management

Missing Controls

Missing or Partially Implemented Controls
Ports, Protocols and Services
ICMP policy
IPv6 Address Filtering
uRPF
SYN Flooding Protection
Device Management
In-Band Management
Device Monitoring
SNMP
Switches, VLANs
VLANs
VLAN Trunking
VLAN Port Security
VLAN Management Policy Server
VPN
Host-to-Host

Vulnerabilities

1. Unauthorized Access
2. Credential Harvesting
3. Breach of Confidentiality
4. ICMP Vulnerabilities
5. SYN Flooding
6. IP Address Spoofing

Potential Threats

1. Network-Related Attacks
2. Compromised Network Node
3. Denial of Service
4. Malicious or Suspicious Traffic
5. Intelligence and Information Gathering

Risk

- Attackers can easily understand network topology and scan for vulnerable versions or Operating Systems using recon and scanning tools. Additionally they can perform DDoS attacks because ICMP echo requests are not disabled.
- Attackers can abuse the lack of source IP check to spoof their source IP address to match the IP address of an internal device, leading to security compromises.

- Since Cloudfare is deployed for DDoS mitigation, only internal attacks need to be mentioned - an attacker with internal network access or a compromised network node can perform SYN flood attacks leading to Denial of Service.
- Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view LDAP credentials in cleartext.
- The DES key used for encryption in SNMPv2 can be cracked with enough time, leading to malicious network activity and network disruption.
- None - VLAN infrastructure not needed
- Not using host-to-host VPN when possible can be abused by attacker with network access to potentially view traffic or at least IP addresses and some additional information depending on the OSI Layer the VPN provides security for.

4. Database Security Risk Management Implementation Controls and Policies

a. Authentication – User accounts
b. Authorization
c. Confidentiality
d. Data Integrity
e. Auditing
f. Replication and Federation
g. Clustering
h. Backup and Recovery
i. OS Protections
j. Application protections
k. Network protections
l. Security Design and Configuration
m. Enclave and Computing environment
n. Business Continuity
o. Vulnerability and Incident management

Missing Controls

Missing or Partially Implemented Controls
Authentication – User accounts
App User Manager
DB Operator
Certificates
Authorization
Rename Default Accounts
Replication and Federation
Federated Databases
Clustering
Clustering Logs

Application Protections
Least Privilege
Network Protections
Time and Count Restrictions
Security Design and Configuration
Policy Review
Application Partitioning
Configuration Management
IA Documentation
System State Changes
Security Identification and Authentication
Group Identification and Authentication
Token and Certificate Standards
Enclave and Computing Environment
Access for Need-to-Know
Encryption – Data in Transit
Audit Security Label Changes
Logon Restrictions
Least Privilege
Enclave Boundary Defense
Business Continuity
Backup Copies of Critical Software
Trusted Recovery

Vulnerabilities

1. Unauthorized Access
2. Credential Harvesting
3. Breach of Confidentiality
4. Uncapped TTL and Session Count
5. Unlimited Logon Attempts
6. Loss or Corruption of Software
7. No Integrity Validation
8. Outdated Policies
9. Unpartitioned Apps
10. Software Library Vulnerabilities
11. Weak Access Control
12. Weak Authentication
13. Impersonation
14. Username Enumeration
15. No Load Balancing

Potential Threats

1. Network-Related Attacks
2. Compromised Network Node
3. Malicious Changes
4. System Error
5. Human Error
6. Natural Disaster

Risk

- Attackers can gain unauthorized access to DB which leads to a breach in confidentiality, and more potentially depending on the level of access the account they are using has.
- Keeping default account names makes it easier for attackers to guess the account name correctly and in turn makes it easier to brute-force the login.
- Without Federated Databases, there will be some issues with handling large volumes of traffic because the load balancing capabilities of federated databases is not being utilized, which could lead to Denial of Service and high latency.
- Lack of logging denies any accountability and effects the integrity of pushed transactions or changes. You also cannot trace things back in the event of a compromise.
- Compromised account or disgruntled employee can perform actions they should not be able to.
- Uncapped session TTL and count can lead to session hijacking attacks as well as denial of service attacks on the DB by flooding it with requests.
- Some policies might become outdated if not reviewed periodically and might cause some problems with compliance and audits.
- Unpartitioned Applications occupying same disk space or server can affect each other if one gets compromised.
- Software Libraries can be modified to contain malicious code if not well maintained.
- Outdated policies and IR playbooks can slow down Incident Response and recovery.
- Allowing group authentication without doing a secondary individual authentication check increases the risk that an unauthorized user or compromised account breaks confidentiality and integrity.
- Access should only be given on a need-to-know basis, or else there could be a privacy violation and breach of confidentiality
- Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view login credentials or other data in cleartext.
- Unlimited Logon Attempts makes the system weak against brute-forcing attacks and potential Denial of Service attacks by login request flooding.
- Lack of protection against unauthorized login attempts due to the lack of network location check for the authenticating user.
- System errors or physical disruptions can lead to the loss of critical software if not backed up
- Lack of integrity check for the configuration files, data files and other files before DB startup can lead to malicious code execution and more.

5. Application Development Security Risk Management Implementation Controls and Policies

a. Program Management

b. Application Data Handling
c. Authentication
d. Use of Cryptography
e. User Accounts
f. Input Validation
g. Auditing
h. Configuration Management
i. Testing
j. Deployment

Missing Controls

Missing or Partially Implemented Controls
Application Data Handling
In-Memory Data Handling
Data Transmission
Authentication
User Authentication
Signed Code Identification
Input Validation
Race Conditions Defenses
Testing
Fuzzy Testing

Vulnerabilities

1. Unauthorized Access
2. Credential Harvesting
3. Breach of Confidentiality
4. No Integrity Validation
5. Weak Authentication
6. Virtual Memory Vulnerabilities
7. Software and Coding Vulnerabilities.

Potential Threats

1. Network-Related Attacks
2. Compromised Network Node
3. Malicious Changes
4. Human Error
5. Compromised Workstation
6. Virtual Memory Attacks
7. Application Attacks

Risk

- Not clearing RAM or virtual memory can lead to code re-use attacks, or just data and code leakage in the case of a compromised system, which is a breach of confidentiality and help attackers in intel gathering.
- Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view login credentials or other data in cleartext.
- Attackers can gain unauthorized access to the app which leads to a breach in confidentiality, and more potentially depending on the level of access the account they compromise has.
- Attackers can potentially make unwanted and malicious changes to code leadings malicious code execution and more.
- Not following best security practices when coding can lead to successful attacks against apps.
- Coding errors and security loopholes will go unnoticed and can lead to successful app layer attacks.

6. Wireless Security Risk Management Implementation Controls and Policies

a. Wireless LAN Risk Management
b. Wireless PAN Risk Management
c. Wireless WAN Risk Management
d. Wireless RFID Risk Management
e. Wireless PED Risk Management

Missing Controls

Missing or Partially Implemented Controls
Wireless LAN Risk Management
EAP-TTLS
PEAP
SSID Protection
Wireless PAN Risk Management
Bluetooth Security Mode
Bluetooth Pairing Security
Wireless WAN Risk Management
Legacy PDA Wireless Air Interface Protocols:
Cellular Digital Packet Data (CDPD)
Mobitex
IEEE 802.16 BWA
IEEE 802.16e
Wireless RFID Risk Management
Active RFID
Wireless PED Risk Management
NSA Type-1 certified tech
Secure Wireless Email
Secure Wireless PDA

Vulnerabilities

1. Unauthorized Access
2. Weak Authentication
3. Weak Encryption
4. Network Device Publicly Discoverable

Potential Threats

1. Network-Related Attacks
2. Compromised Network Node
3. Disgruntled Employee
4. Lost RFID tag
5. Malicious Actor

Risk

- Not using identity hiding which is one of the benefits of EAP-TTLS, so the authenticator is aware of both the username that establishes the TLS channel in the first phase and the user authenticated in the second phase
- Attacker knows SSID of the router as it is discoverable, so he can perform different attacks and gain intel on the network's security posture. The attacker can also spoof access points SSID to trick guests.
- Someone with physical access to a workstation that uses bluetooth can take advantage of some weak authentication methods.
- Someone with access to an RFID tag can attempt to read data stored if it not well encrypted - passive RFID has weaker encryption than active RFID because the latter uses a battery.

7. Across all Security Risk areas 1-6 from above provide a table for:

a. List of Cybersecurity Implementation controls that exist at your company

Access Control Security Risk Management Implementation Controls and Policies

Implementation Controls
Identification Credentials
Username/UserID
Password
ID Card
Personal Authentication
Password
Smart Card/Private Key/ Token
Single or Multi-Factor Authentication
Access Control Lists
Policies
Authorization

Access Control Lists
Smart Card/Security Token
Deny-By-Default Policy
Logical Access Control Methods
Network Architecture Controls
Remote Network Access
Securing Network Ports
Physical Security for SIPRNeT Ports
Logical Network Port Security
Port Authentication Using 802.1X
Network Access Control (NAC) Systems
Encryption
Passwords and PINs
Physical Access Control Methods
Classified Storage and Handling
Badges
PINs and Combinations
Physical Intrusion Detection Systems

Network Infrastructure Security Risk Management Implementation Controls and Policies

Implementation Controls
Enclave Protection
Defense-in-Depth
Firewalls
Routers
IDS
IPS
Encryption
DMZ
Backdoor Protection
VPN Tunnel
Firewalls
Packet Filtering
Deep Packet Inspection
Application Proxy Gateway
Hybrid Technology Firewalls
Proxy Servers
Layered Firewall Architecture
Routers
Route Table Integrity

Static Routes
Neighbor Router Authentication
Securing Router Planes

Network Infrastructure Management Security Risk Management Implementation Controls and Policies

Implementation Controls
Ports, Protocols and Services
Default Deny Port Policy
IPv4 Address Filtering
SYN Flooding Protection
Device Management
Device and Asset Management
Out-of-Band Management
Device Monitoring
SNMP
Network Management Station
Network Authentication, Authorization and Accounting
Network Authentication
Network Authorization
Network Accounting
AAA
Syslog Servers
Local Accounts
Router Password Protection
NIDS
External Network Intrusion Detection
Local Area Network Intrusion Detection
Switches, VLANs
Physical Switch Security
802.1X
VPN
Gateway-to-Gateway
Host-to-Gateway

Database Security Risk Management Implementation Controls and Policies

Implementation Controls
Authentication – User accounts
Application User
DB Admin

App Owner
App Account
DB Auditor
Passwords
External Authentication
Credential Storage
Authorization
RBAC
Rename Default Accounts
Confidentiality
Data Encryption
Data File Encryption
Application Code
Data Integrity
Transaction Logs
Redundancy Policies
Auditing
Audit Logs Protection
Audit Logs Retention
Audit Reporting
Replication and Federation
Database Links
Database Replication
Clustering
Database Clustering
Encryption
Backup and Recovery
DBMS Backup
Testing
Encryption
OS Protections
Dedicated Database Partitions
Dedicated OS Account
DB Software
Application Protections
Input Validation
Authentication
Network Protections
Network Access Restrictions

Encryption
Security Design and Configuration
Policy Review
Configuration Specifications
Compliance Testing
Functional Architecture for IS applications
Non-Repudiation
Application Partitioning
Ports, Protocols, and Services
IA Documentation
Security Support Structure Partitioning
Security Identification and Authentication
Group Identification and Authentication
Individual Identification and Authentication
Key Management
Enclave and Computing Environment
Access for Need-to-Know
Audit Trail, Monitoring, Analysis and Reporting
Changes to Data
Encryption – Data at Rest
Data Change Controls
Business Continuity
Protection of Backup and Restoration Assets
Disaster and Recovery Planning
Backup Copies of Critical Software
Vulnerability and Incident Management
Vulnerability Management

Applications Development Security Risk Management Implementation Controls and Policies

Implementation Controls
Application Data Handling
Database Management System
Data Storage
Data Integrity
Data Marking
Authentication
Server Authentication
Standalone Application Authentication
Server Application Authentication
Client Application Authentication

Combination Client Server Application Authentication
Application Component Authentication
PKI Certificate Validation
Password Complexity and Maintenance
Authentication Credentials Protection
Use of Cryptography
Symmetric Ciphers
Tampering Controls
Data Authentication
Data at rest
User Accounts
Account Management
Application Session Policies
Access Control
Input Validation
Static Analysis Tool
Validate User Input
SQL Injection Defenses
Integer Overflows Defenses
Format String Defenses
Buffer Overflow Defenses
Auditing
User Notifications
Audit Trail Protection
Configuration Management
Software Configuration Management
Release Manager
Testing
Automated Tools
Web App Security
Deployment
Deployment Documentation

Wireless Security Risk Management Implementation Controls and Policies

Implementation Controls
Wireless LAN Risk Management
IEEE 802.11x EAP
EAP-TLS
Network Separation

WPA2 Protocol
IPSec
WTLS
Wireless PAN Risk Management
IEEE 802.15
Wireless RFID Risk Management
Passive RFID

b. Comparison of the Implementation controls discussed in class with your company's existing Cybersecurity Implementation controls

Implementation Controls	**Status: Fully, Partially or Not Implemented**
Identification Credentials	
Username/UserID	Fully Implemented
Password	Fully Implemented
Pin Code	Not Implemented
PKI Certificate/Digital Signature	Not Implemented
ID Card	Partially Implemented
Photograph	Not Implemented
Biometric Authentication	Not Implemented
Personal Authentication	
Password	Fully Implemented
Smart Card/Private Key/ Token	Partially Implemented
Biometric	Not Implemented
Single or Multi-Factor Authentication	Fully Implemented
Access Control Lists	Fully Implemented
Policies	Fully Implemented
Authorization	
Access Control Lists	Fully Implemented
Smart Card/Security Token	Partially Implemented
Deny-By-Default Policy	Fully Implemented
Logical Access Control Methods	
Network Architecture Controls	Partially Implemented
Remote Network Access	Fully Implemented
Securing Network Ports	Fully Implemented
Physical Security for SIPRNeT Ports	Fully Implemented
Logical Network Port Security	Fully Implemented
Port Authentication Using 802.1X	Fully Implemented
Network Access Control (NAC) Systems	Fully Implemented

Encryption	Partially Implemented
PKI Compliance Requirements	Not Implemented
Passwords and PINs	Fully Implemented
Physical Tokens	Not Implemented
Alternate Login Tokens	Not Implemented
Physical Access Control Methods	
Classified Storage and Handling	Fully Implemented
Defense Biometric Identification System	Not Implemented
Badges	Partially Implemented
Memory Cards	Not Implemented
Smart Cards	Not Implemented
PINs and Combinations	Fully Implemented
Physical Tokens	Not Implemented
Physical Intrusion Detection Systems	Fully Implemented
Biometric Systems	
Fingerprint Scanner	Not Implemented
Facial Recognition System	Not Implemented
Enclave Protection	
Defense-in-Depth	Fully Implemented
Firewalls	Fully Implemented
Routers	Fully Implemented
IDS	Fully Implemented
IPS	Fully Implemented
Encryption	Partially Implemented
DMZ	Fully Implemented
Network Test Access Ports (TAP)	Not Implemented
Backdoor Protection	Fully Implemented
VPN Tunnel	Fully Implemented
Firewalls	
Packet Filtering	Fully Implemented
Bastion Host	Not Implemented
Stateful Inspection	Not Implemented
Deep Packet Inspection	Fully Implemented
Application Proxy Gateway	Fully Implemented
Hybrid Technology Firewalls	Fully Implemented
Proxy Servers	Fully Implemented
Layered Firewall Architecture	Fully Implemented
Routers	

Route Table Integrity	Fully Implemented
Static Routes	Fully Implemented
Neighbor Router Authentication	Fully Implemented
Securing Router Planes	Partially Implemented
Ports, Protocols and Services	
Default Deny Port Policy	Fully Implemented
ICMP policy	Not Implemented
IPv4 Address Filtering	Fully Implemented
IPv6 Address Filtering	Not Implemented
uRPF	Not Implemented
SYN Flooding Protection	Partially Implemented
Device Management	
Device and Asset Management	Fully Implemented
Out-of-Band Management	Fully Implemented
In-Band Management	Not Implemented
Device Monitoring	
SNMP	Partially Implemented
Network Management Station	Fully Implemented
Network Authentication, Authorization and Accounting	
Network Authentication	Fully Implemented
Network Authorization	Fully Implemented
Network Accounting	Fully Implemented
AAA	Fully Implemented
Syslog Servers	Fully Implemented
Local Accounts	Fully Implemented
Router Password Protection	Fully Implemented
NIDS	
External Network Intrusion Detection	Fully Implemented
Local Area Network Intrusion Detection	Fully Implemented
Switches, VLANs	
Physical Switch Security	Fully Implemented
VLANs	Not Implemented
VLAN Trunking	Not Implemented
VLAN Port Security	Not Implemented
802.1X	Fully Implemented
VLAN Management Policy Server	Not Implemented

VPN	
Gateway-to-Gateway	Fully Implemented
Host-to-Gateway	Fully Implemented
Host-to-Host	Not Implemented
Authentication – User accounts	
Application User	Fully Implemented
DB Admin	Fully Implemented
App Owner	Fully Implemented
App User Manager	Not Implemented
App Account	Fully Implemented
DB Auditor	Fully Implemented
DB Operator	Not Implemented
Passwords	Fully Implemented
Certificates	Not Implemented
External Authentication	Fully Implemented
Credential Storage	Fully Implemented
Authorization	
RBAC	Fully Implemented
Rename Default Accounts	Partially Implemented
Confidentiality	
Data Encryption	Fully Implemented
Data File Encryption	Fully Implemented
Application Code	Fully Implemented
Data Integrity	
Transaction Logs	Fully Implemented
Redundancy Policies	Fully Implemented
Auditing	
Audit Logs Protection	Fully Implemented
Audit Logs Retention	Fully Implemented
Audit Reporting	Fully Implemented
Replication and Federation	
Database Links	Fully Implemented
Database Replication	Fully Implemented
Federated Databases	Not Implemented
Clustering	
Database Clustering	Fully Implemented
Clustering Logs	Not Implemented

Encryption	Fully Implemented
Backup and Recovery	
DBMS Backup	Fully Implemented
Testing	Fully Implemented
Encryption	Fully Implemented
OS Protections	
Dedicated Database Partitions	Fully Implemented
Dedicated OS Account	Fully Implemented
DB Software	Fully Implemented
Application Protections	
Input Validation	Fully Implemented
Authentication	Fully Implemented
Least Privilege	Not Implemented
Network Protections	
Network Access Restrictions	Fully Implemented
Time and Count Restrictions	Not Implemented
Encryption	Fully Implemented
Security Design and Configuration	
Policy Review	Partially Implemented
Configuration Specifications	Fully Implemented
Compliance Testing	Fully Implemented
Functional Architecture for IS applications	Fully Implemented
Non-Repudiation	Fully Implemented
Application Partitioning	Partially Implemented
Ports, Protocols, and Services	Fully Implemented
Configuration Management	Not Implemented
IA Documentation	Partially Implemented
Security Support Structure Partitioning	Fully Implemented
System State Changes	Not Implemented
Security Identification and Authentication	
Group Identification and Authentication	Partially Implemented
Individual Identification and Authentication	Fully Implemented
Key Management	Fully Implemented
Token and Certificate Standards	Not Implemented
Enclave and Computing Environment	
Access for Need-to-Know	Partially Implemented
Audit Trail, Monitoring, Analysis and Reporting	Fully Implemented

Changes to Data	Fully Implemented
Encryption – Data at Rest	Fully Implemented
Encryption – Data in Transit	Not Implemented
Data Change Controls	Fully Implemented
Audit Security Label Changes	Not Implemented
Logon Restrictions	Not Implemented
Least Privilege	Not Implemented
Enclave Boundary Defense	Not Implemented
Business Continuity	
Protection of Backup and Restoration Assets	Fully Implemented
Disaster and Recovery Planning	Fully Implemented
Backup Copies of Critical Software	Partially Implemented
Trusted Recovery	Not Implemented
Vulnerability and Incident Management	
Vulnerability Management	Fully Implemented
Application Data Handling	
Database Management System	Fully Implemented
Data Storage	Fully Implemented
In-Memory Data Handling	Not Implemented
Data Transmission	Not Implemented
Data Integrity	Fully Implemented
Data Marking	Fully Implemented
Authentication	
Server Authentication	Fully Implemented
User Authentication	Not Implemented
Signed Code Identification	Not Implemented
Standalone Application Authentication	Fully Implemented
Server Application Authentication	Fully Implemented
Client Application Authentication	Fully Implemented
Combination Client Server Application Authentication	Fully Implemented
Application Component Authentication	Fully Implemented
PKI Certificate Validation	Fully Implemented
Password Complexity and Maintenance	Fully Implemented
Authentication Credentials Protection	Fully Implemented
Use of Cryptography	
Symmetric Ciphers	Fully Implemented

Tampering Controls	Fully Implemented
Data Authentication	Fully Implemented
Data at rest	Fully Implemented
User Accounts	
Account Management	Fully Implemented
Application Session Policies	Fully Implemented
Access Control	Fully Implemented
Input Validation	
Static Analysis Tool	Fully Implemented
Validate User Input	Fully Implemented
SQL Injection Defenses	Fully Implemented
Integer Overflows Defenses	Fully Implemented
Format String Defenses	Fully Implemented
Buffer Overflow Defenses	Fully Implemented
Race Conditions Defenses	Not Implemented
Auditing	
User Notifications	Fully Implemented
Audit Trail Protection	Fully Implemented
Configuration Management	
Software Configuration Management	Fully Implemented
Release Manager	Fully Implemented
Testing	
Fuzzy Testing	Not Implemented
Automated Tools	Fully Implemented
Web App Security	Fully Implemented
Deployment	
Deployment Documentation	Fully Implemented
Wireless LAN Risk Management	
IEEE 802.11x EAP	Fully Implemented
EAP-TLS	Fully Implemented
EAP-TTLS	Not Implemented
PEAP	Not Implemented
Network Separation	Fully Implemented
WPA2 Protocol	Fully Implemented
IPSec	Fully Implemented
WTLS	Fully Implemented
SSID Protection	Not Implemented

Wireless PAN Risk Management	
IEEE 802.15	Fully Implemented
Bluetooth Security Mode	Not Implemented
Bluetooth Pairing Security	Not Implemented
Wireless WAN Risk Management	
Legacy PDA Wireless Air Interface Protocols:	
Cellular Digital Packet Data (CDPD)	Not Implemented
Mobitex	Not Implemented
IEEE 802.16 BWA	Not Implemented
IEEE 802.16e	Not Implemented
Wireless RFID Risk Management	
Passive RFID	Fully Implemented
Active RFID	Not Implemented
Wireless PED Risk Management	
NSA Type-1 certified tech	Not Implemented
Secure Wireless Email	Not Implemented
Secure Wireless PDA	Not Implemented

c. List of critical assets that exist in your company

S.No.	Asset Type	Value ($)
A1	Financial Resources	$100,000,000
A2	Client Investments	$70,000,000,000
A3	Client and Personnel Information	$50,000,000
A4	Network and Operations Systems	$10,000,000
A5	Business and IT Software/Apps	$3,000,000
A6	Client's Trust	Intangible
A7	Reputation	Intangible

d. List of potential vulnerabilities for critical assets where Cybersecurity Implementation Controls are missing

Missing or Partially Implemented Controls	Vulnerability
Identification Credentials	
Pin Code	Impersonation
PKI Certificate/Digital Signature	Repudiation and Weak Authentication

ID Card	Unauthorized Access
Photograph	Impersonation and Weak Authentication
Biometric Authentication	Impersonation
Personal Authentication	
Smart Card/Private Key/ Token	Unauthorized Access and Weak Authentication
Biometric	Impersonation
Authorization	
Smart Card/Security Token	Unauthorized Access
Logical Access Control Methods	
Network Architecture Controls	Network-Related Attacks
Encryption	Network-Related Attacks and Breach of Confidentiality and Integrity
PKI Compliance Requirements	Repudiation and Weak Authentication
Physical Tokens	Impersonation and Weak Authentication
Alternate Login Tokens	None
Physical Access Control Methods	
Defense Biometric Identification System	Impersonation
Badges	Unauthorized Access
Memory Cards	Impersonation
Smart Cards	Impersonation
Physical Tokens	Unauthorized Access and Weak Authentication
Biometric Systems	
Fingerprint Scanner	Impersonation
Facial Recognition System	Impersonation
Enclave Protection	
Encryption	Unauthorized Access + Credential Harvesting
Network Test Access Ports (TAP)	Network congestion + Poor IDS/IPS Performance
Firewalls	
Bastion Host	None (Deep Packet Inspection Firewall covers capabilities)
Stateful Inspection	None (Deep Packet Inspection Firewall covers capabilities)
Routers	
Securing Router Planes	Weak Protection against recon and scanning tools
Ports, Protocols and Services	
ICMP policy	ICMP Vulnerabilities
IPv6 Address Filtering	None - IPv6 not deployed
uRPF	IP address spoofing
SYN Flooding Protection	SYN Flooding

Device Management	
In-Band Management	Unauthorized Access + Credential Harvesting
Device Monitoring	
SNMP	Unauthorized Access
Switches, VLANs	
VLANs	None - VLAN infrastructure not needed
VLAN Trunking	None - VLAN infrastructure not needed
VLAN Port Security	None - VLAN infrastructure not needed
VLAN Management Policy Server	None - VLAN infrastructure not needed
VPN	
Host-to-Host	Breach of Confidentiality
Authentication – User accounts	
App User Manager	None - DBA manages users
DB Operator	None - DBA does not need assistance
Certificates	Weak Authentication + Unauthorized Access
Authorization	
Rename Default Accounts	Username Enumeration
Replication and Federation	
Federated Databases	No Load Balancing
Clustering	
Clustering Logs	No Integrity Validation
Application Protections	
Least Privilege	Unauthorized Access + Weak Access Control
Network Protections	
Time and Count Restrictions	Session Hijacking + Denial of Service
Security Design and Configuration	
Policy Review	Outdated Policies
Application Partitioning	Unpartitioned Apps
Configuration Management	Software Library Vulnerabilities
IA Documentation	Outdated Policies
System State Changes	No Integrity Validation
Security Identification and Authentication	
Group Identification and Authentication	Weak Authentication + Unauthorized Access
Token and Certificate Standards	Weak Authentication + Unauthorized Access
Enclave and Computing Environment	
Access for Need-to-Know	Breach of Confidentiality
Encryption – Data in Transit	Unauthorized Access + Credential Harvesting

Audit Security Label Changes	No Integrity Validation
Logon Restrictions	Unlimited Logon Attempts
Least Privilege	Unauthorized Access + Weak Access Control
Enclave Boundary Defense	Unauthorized Access + Impersonation
Business Continuity	
Backup Copies of Critical Software	Loss or Corruption of Software
Trusted Recovery	No Integrity Validation
Application Data Handling	
In-Memory Data Handling	Breach of Confidentiality + Virtual Memory Vulns
Data Transmission	Unauthorized Access + Credential Harvesting
Authentication	
User Authentication	Unauthorized Access + Weak Authentication
Signed Code Identification	No Integrity Validation
Input Validation	
Race Conditions Defenses	Software and Coding vulnerabilities
Testing	
Fuzzy Testing	Software and Coding vulnerabilities
Wireless LAN Risk Management	
EAP-TTLS	Weak Authentication + Unauthorized Access
PEAP	Weak Authentication + Unauthorized Access
SSID Protection	Network Device Publicly Discoverable
Wireless PAN Risk Management	
Bluetooth Security Mode	Weak Authentication + Unauthorized Access
Bluetooth Pairing Security	Weak Authentication + Unauthorized Access
Wireless WAN Risk Management	
Legacy PDA Wireless Air Interface Protocols:	
Cellular Digital Packet Data (CDPD)	None - no WWAN implementations exist
Mobitex	None - no WWAN implementations exist
IEEE 802.16 BWA	None - no WWAN implementations exist
IEEE 802.16e	None - no WWAN implementations exist
Wireless RFID Risk Management	
Active RFID	Weak Encryption
Wireless PED Risk Management	
NSA Type-1 certified tech	None - Wireless PED not allowed
Secure Wireless Email	None - Wireless PED not allowed
Secure Wireless PDA	None - Wireless PED not allowed

e. List of potential threats to your company that could exploit vulnerabilities of critical assets

Vulnerability	Threat
Unauthorized Access	Disclosure of Confidential Information
Impersonation	Intelligence and Information Gathering
Weak Authentication	Financial Theft
Repudiation	Loss of Accountability and Trust
Network-Related Vulnerabilities	Network-Related Attacks
Breach of Confidentiality and Integrity	Disclosure of Confidential Information
Unauthorized Access	Network-Related Attacks
Credential Harvesting	Compromised Network Node
Network Congestion	Denial of Service
Poor IDS/IPS Performance	Malicious or Suspicious Traffic
Weak Protection against Recon and Scanning Tools	Intelligence and Information Gathering
Breach of Confidentiality	Compromised Network Node
ICMP Vulnerabilities	Intelligence and Information Gathering
SYN Flooding	Denial of Service
IP Address Spoofing	Malicious or Suspicious Traffic
Uncapped TTL and Session Count	Compromised Network Node
Unlimited Logon Attempts	Compromised Network Node
Loss or Corruption of Software	Natural Disaster + System Error
No Integrity Validation	Malicious Changes + Human Error
Outdated Policies	Malicious Changes
Unpartitioned Apps	Compromise Spread
Software Library Vulnerabilities	Malicious Changes
Weak Access Control	Compromised Network Node
Weak Authentication	Compromised Network Node
Impersonation	Compromised Network Node
Username Enumeration	Compromised Network Node
No Load Balancing	Compromised Network Node
Virtual Memory Vulnerabilities	Compromised Workstation + Virtual Memory Attacks
Software and Coding Vulnerabilities.	Compromised Workstation + App attacks
Unauthorized Access	Network-Related Attacks + Compromised Network Node
Weak Encryption	Disgruntled Employee + Lost RFID tag
Network Device Publicly Discoverable	Network-Related Attacks + Malicious Actor

List of Unique Threats

1. App attacks
2. Compromise Spread

3. Compromised Network Node
4. Compromised Workstation
5. Denial of Service
6. Disclosure of Confidential Information
7. Disgruntled Employee
8. Financial Theft
9. Human Error
10. Intelligence and Information Gathering
11. Loss of Accountability and Trust
12. Lost RFID tag
13. Malicious Actor
14. Malicious Changes
15. Malicious or Suspicious Traffic
16. Natural Disaster
17. Network-Related Attacks
18. System Error
19. Virtual Memory Attacks

f. List of potential risks for critical assets where Cybersecurity Implementation Controls are missing

Missing or Partially Implemented Controls	**Risk**
Identification Credentials	
PIN Code	No significant risk due to lack of PIN code for identification
PKI Certificate/Digital Signature	Attackers can leverage repudiation and in the case of email communications, interception of messages is possible leading to a breach in confidentiality and to a loss of trust
ID Card	RFID card can be stolen or potentially duplicated to provide access to unauthorized individuals
Photograph	Does not match ID card to a face, leading to potential impersonation and to unauthorized access
Biometric Authentication	Identity theft not put in check, leading to potential impersonation and to unauthorized access
Personal Authentication	
Smart Card/Private Key/ Token	RFID card can be stolen or potentially duplicated to provide access to unauthorized individuals
Biometric	Identity theft not put in check, leading to potential impersonation and to unauthorized access
Authorization	
Smart Card/Security Token	RFID card can be stolen or potentially duplicated to provide access to unauthorized individuals
Logical Access Control Methods	

Network Architecture Controls	Use of outdated network protocols can lead to successful network-related attacks, compromising integrity of the information systems as well as the confidentiality of data flowing across the network
Encryption	Weak LAN encryption for network services can reveal user credentials to potential packet sniffing on the LAN, giving attackers access to IT systems and apps
PKI Compliance Requirements	Attackers can leverage repudiation and integrity verification weaknesses and in the case of email communications, interception of messages is possible leading to a breach in confidentiality and to a loss of trust
Physical Tokens	Might lead to weak authentication, which can grant unauthorized access
Alternate Login Tokens	No significant risk due to lack of alternate login tokens
Physical Access Control Methods	
Defense Biometric Identification System	Identity theft not put in check, leading to potential impersonation and to unauthorized access of physical assets and resources.
Badges	Weak authentication that can lead to potential impersonation and to unauthorized access of physical assets and resources.
Memory Cards	Weak authentication that can lead to potential impersonation and to unauthorized access of physical assets and resources.
Smart Cards	Weak authentication that can lead to potential impersonation and to unauthorized access of physical assets and resources.
Physical Tokens	Might lead to weak authentication, which can grant unauthorized access
Biometric Systems	
Fingerprint Scanner	Identity theft not put in check, leading to potential impersonation and to unauthorized access of logical and physical assets and resources.
Facial Recognition System	Identity theft not put in check, leading to potential impersonation and to unauthorized access of logical and physical assets and resources.
Enclave Protection	
Encryption	Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view LDAP credentials in cleartext
Network Test Access Ports (TAP)	Lack of NTAP can lead to traffic congestion and delays due to IDS working in real-time and not on

	duplicate/mirrored packets, which can potentially lead to loss of services availability.
Firewalls	
Bastion Host	Deep Inspection Firewalls are already configured and cover all of this firewall's capabilities
Stateful Inspection	Deep Inspection Firewalls are already configured and cover all of this firewall's capabilities
Routers	
Securing Router Planes	Attackers can easily understand network topology and scan for vulnerable versions or Operating Systems using recon and scanning tools. Additionally they can perform DDoS attacks because ICMP echo requests are not disabled.
Ports, Protocols and Services	
ICMP policy	Attackers can easily understand network topology and scan for vulnerable versions or Operating Systems using recon and scanning tools. Additionally they can perform DDoS attacks because ICMP echo requests are not disabled.
IPv6 Address Filtering	None - IPv6 not being used.
uRPF	Attackers can abuse the lack of source IP check to spoof their source IP address to match the IP address of an internal device, leading to security compromises.
SYN Flooding Protection	Since Cloudfare is deployed for DDoS mitigation, only internal attacks need to be mentioned - an attacker with internal network access or a compromised network node can perform SYN flood attacks leading to Denial of Service.
Device Management	
In-Band Management	Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view LDAP credentials in cleartext.
Device Monitoring	
SNMP	The DES key used for encryption in SNMPv2 can be cracked with enough time, leading to malicious network activity and network disruption.
Switches, VLANs	
VLANs	None - VLAN infrastructure not needed
VLAN Trunking	None - VLAN infrastructure not needed
VLAN Port Security	None - VLAN infrastructure not needed
VLAN Management Policy Server	None - VLAN infrastructure not needed

VPN	
Host-to-Host	Not using host-to-host VPN when possible can be abused by attacker with network access to potentially view traffic or at least IP addresses and some additional information depending on the OSI Layer the VPN provides security for.
Authentication – User accounts	
App User Manager	None - DBA manages users
DB Operator	None - DBA does not need assistance
Certificates	Attackers can gain unauthorized access to DB which leads to a breach in confidentiality, and more potentially depending on the level of access the account they are using has.
Authorization	
Rename Default Accounts	Keeping default account names makes it easier for attackers to guess the account name correctly and in turn makes it easier to brute-force the login.
Replication and Federation	
Federated Databases	Without Federated Databases, there will be some issues with handling large volumes of traffic because the load balancing capabilities of federated databases is not being utilized, which could lead to Denial of Service and high latency.
Clustering	
Clustering Logs	Lack of logging denies any accountability and effects the integrity of pushed transactions or changes. You also cannot trace things back in the event of a compromise.
Application Protections	
Least Privilege	Compromised account or disgruntled employee can perform actions they should not be able to.
Network Protections	
Time and Count Restrictions	Uncapped session TTL and count can lead to session hijacking attacks as well as denial of service attacks on the DB by flooding it with requests.
Security Design and Configuration	
Policy Review	Some policies might become outdated if not reviewed periodically and might cause some problems with compliance and audits.
Application Partitioning	Unpartitioned Applications occupying same disk space or server can affect each other if one gets compromised.
Configuration Management	Software Libraries can be modified to contain malicious code if not well maintained.

IA Documentation	Outdated policies and IR playbooks can slow down Incident Response and recovery.
System State Changes	Lack of logging denies any accountability and effects the integrity of pushed transactions or changes. You also cannot trace things back in the event of a compromise.
Security Identification and Authentication	
Group Identification and Authentication	Allowing group authentication without doing a secondary individual authentication check increases the risk that an unauthorized user or compromised account breaks confidentiality and integrity.
Token and Certificate Standards	Attackers can gain unauthorized access to DB which leads to a breach in confidentiality, and more potentially depending on the level of access the account they are using has.
Enclave and Computing Environment	
Access for Need-to-Know	Access should only be given on a need-to-know basis, or else there could be a privacy violation and breach of confidentiality
Encryption – Data in Transit	Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view login credentials or other data in cleartext.
Audit Security Label Changes	Lack of logging denies any accountability and effects the integrity of pushed transactions or changes. You also cannot trace things back in the event of a compromise.
Logon Restrictions	Unlimited Logon Attempts makes the system weak against brute-forcing attacks and potential Denial of Service attacks by login request flooding.
Least Privilege	Compromised account or disgruntled employee can perform actions they should not be able to.
Enclave Boundary Defense	Lack of protection against unauthorized login attempts due to the lack of network location check for the authenticating user.
Business Continuity	
Backup Copies of Critical Software	System errors or physical disruptions can lead to the loss of critical software if not backed up
Trusted Recovery	Lack of integrity check for the configuration files, data files and other files before DB startup can lead to malicious code execution and more.
Application Data Handling	

In-Memory Data Handling	Not clearing RAM or virtual memory can lead to code re-use attacks, or just data and code leakage in the case of a compromised system, which is a breach of confidentiality and help attackers in intel gathering.
Data Transmission	Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view login credentials or other data in cleartext.
Authentication	
User Authentication	Attackers can gain unauthorized access to the app which leads to a breach in confidentiality, and more potentially depending on the level of access the account they compromise has.
Signed Code Identification	Attackers can potentially make unwanted and malicious changes to code leadings malicious code execution and more.
Input Validation	
Race Conditions Defenses	Not following best security practices when coding can lead to successful attacks against apps.
Testing	
Fuzzy Testing	Coding errors and security loopholes will go unnoticed and can lead to successful app layer attacks.
Wireless LAN Risk Management	
EAP-TTLS	Not using identity hiding which is one of the benefits of EAP-TTLS, so the authenticator is aware of both the username that establishes the TLS channel in the first phase and the user authenticated in the second phase
PEAP	Similar to EAP-TTLS risk
SSID Protection	Attacker knows SSID of the router as it is discoverable, so he can perform different attacks and gain intel on the network's security posture. The attacker can also spoof access points SSID to trick guests.
Wireless PAN Risk Management	
Bluetooth Security Mode	Someone with physical access to a workstation that uses bluetooth can take advantage of some weak authentication methods.
Bluetooth Pairing Security	Someone with physical access to a workstation that uses bluetooth can take advantage of some weak authentication methods.
Wireless WAN Risk Management	
Legacy PDA Wireless Air Interface Protocols:	
Cellular Digital Packet Data (CDPD)	None - no WWAN implementations exist
Mobitex	None - no WWAN implementations exist
IEEE 802.16 BWA	None - no WWAN implementations exist

IEEE 802.16e	None - no WWAN implementations exist
Wireless RFID Risk Management	
Active RFID	Someone with access to an RFID tag can attempt to read data stored if it not well encrypted - passive RFID has weaker encryption than active RFID because the latter uses a battery.
Wireless PED Risk Management	
NSA Type-1 certified tech	None - Wireless PED not allowed
Secure Wireless Email	None - Wireless PED not allowed
Secure Wireless PDA	None - Wireless PED not allowed

g. List of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks (it is not required to write detailed policies) – Risk Prevention Strategy

- Most important control that needs to be added to HIC's security plan is a PKI infrastructure that will provide non-repudiation and trustworthiness for trade requests or financial transfer requests done on the business end. Additionally, having PKI certificates allows for Multi-Factor Authentication capabilities for login purposes, as well as S/MIME encryption for email communications.
- Instead of using only RFID cards, the use of Smart ID Cards is highly recommended as it displays the user's name and an image of their face.
- To go along with the Smart ID Cards, you either need security personnel to check IDs on building entry, or use a biometric scanner (fingerprint scanning is more advisable than facial recognition as it tends to be quicker and in some cases more secure). It would be even more secure if both of a security check and biometric scanner were used, but that is not very convenient and is can be viewed as overkill.
- Update the configuration of network systems that still use protocols with weak encryption or that are more prone to attacks compared to their updated versions. For instance, move towards LDAPS, DNSSec, TACACS+ and so on.
- Providing users with physical tokens can prove to be very effective, because the use of their PKI certificate isn't bound to the computer only. For instance, if an attacker has access to the user's account, they cannot use the certificate immediately as they need the physical token. Another alternative to protect PKI certificates is to password-protect their use.
- Use of DBIDS is highly advised to protect physical assets or facilities.
- Install Network Access Ports to resolve and processing and congestion issues with IDS solutions
- Configure Unicast Reverse Path Forwarding (uRPF) on routers, which inspects incoming packets' source IP address and checks that it belongs to the interface it is coming from, by referencing the routing table. This is a great method to stop IP address spoofing attacks.
- Restrict the time window and/or the packet rate for an open TCP connection. This can be done on the router by reducing wait time before resetting a connection, and by creating a firewall filter that limits the rate of SYN traffic based on bandwidth utilization as well as maximum burst size.

- Move from SNMPv2 to SNMPv3 as it offers more secure cryptographic suites for encryption, amongst other benefits.
- Configure TLS on DB servers to protect data in transit.
- Restrict Session TTL and session count for DB connections.
- Put logon restrictions in place, such as limited tries before account is locked to protect against DoS or Brute-Forcing attacks.
- Use Federated Databases to handle large volumes of traffic by utilizing the load balancing capabilities it has to offer, which protects against availability attacks.
- Configure TLS or IPSec on app servers to protect app data in-transit.
- Restrict Session TTL and session count for app sessions.
- For users that require app authentication, the mechanism should be DoD PKI credentials, or credentials authorized under the DoD External Certificate Authority (ECA) program.
- Minimize use of global variables, use thread-safe functions and ensure enforcement of ACLs, to protect against race conditions attacks.
- Disable SSID Broadcast on wireless network devices and provide clients and guest network users with SSID after getting approval.
- Configure EAP-TTLS to authenticate client connecting to the network.
- Consider switching to active RFID tags as they offer more secure encryption.

h. List of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks (it is not required to write detailed policies) – Risk Prevention Strategy

- Improve Incident Handling processes by preparing Incident Response Playbooks and categorizing them properly as well as making them easily accessible.
- Update Incident Response Playbooks regularly as the threat landscape and attack surface is always evolving.
- Create and regularly revise a Business Continuity Plan as the clients and the company's mission are the top priority.
- Regularly monitor logs using IDS software that generates alerts, and regularly tune the IDS software to get rid of false positives and identify unauthorized access or suspicious behavior.
- Router should not allow any identification support or finger services, as they both allow for easy intel gathering on a compromised network node.
- Routers should not allow ICMP echo requests which can be used for network discovery and DoS attacks.
- Configure collection of Clustering Logs, System State Changes and Audit Security Label Changes.
- Backup copies of critical software to protect against accidental loss, system errors or other compromises.
- Employ Trusted Recovery to validate the integrity of configuration files, data files, and other files before the DB starts up.

- Improve Incident Handling processes by preparing Incident Response Playbooks and categorizing them properly as well as making them easily accessible.
- Update Incident Response Playbooks regularly as the threat landscape and attack surface is always evolving.
- Clear virtual memory or RAM that previously stored that data.
- Usage of DoD PKI mobile code signing certificate is required to validate integrity and legitimacy of code before executing on a workstation.
- Implement Fuzzy Testing to protect against coding errors and security loopholes.
- Have Bluetooth communications setup on security Mode 4 and to fall back onto security Mode 3 if the former fails.

8. Applicable Government Regulations and Industry Standards discussed in Class 12

a. ISO 17799

ISO 17799 is based on the original British Standard BS 7799, and is a comprehensive standard for Security Risk Management and Assessment, with risk being the key control.

b. ISO 27000 Standard

The ISO27k series of standards provide guidance on designing, implementing and auditing Information Security Management Systems in order to protect the 3 pillars of Information Assurance – Confidentiality, Integrity and Availability of information assets.

c. Gramm-Leach-Bliley Act

The GLB act is known as the Financial Modernization Act of 1999 and it comprises 3 security controls – Financial Privacy, Safeguarding of Data and the Prohibition of Pretexting, which is considered as the deceitful extraction and use of customer data.

d. Sarbanes-Oxley Act

The Sarbanes-Oxley Act is considered one of the most pervasive legislations for financial reporting for US and international corporations. The act is arranged into 11 titles, and the most important ones as far as compliance is concerned are the SOX titles 302, 401, 404, 409, 802 and 906.

e. Federal Red Flags Rules

The Federal Red Flags Rules were implemented in 2009 and they apply to pretty much every business as it presses an organization to develop and implement an Identity Theft Prevention Program, as well as to identify red flags around identity theft and report them to the Government, FBI, Secret Service or local state agencies.

f. Massachusetts Security Plan

The Massachusetts Security Plan applies to any company which stores, maintains, owns or licenses personal information on residents of Massachusetts. This does also include all other states in the US, and potentially all international firms, but it can be difficult to really monitor and enforce this plan worldwide.

9. Rank asset risks and vulnerability risks for your company across Access Control, Network Infrastructure, Network Infrastructure Management, Database, Applications, and Wireless.

Control Family	Top 5 Vulnerabilities	Top 5 Risks
Access Control	1. Unauthorized Access	· Use of outdated network protocols can lead to successful network-related attacks, compromising integrity of the information systems as well as the confidentiality of data flowing across the network
	2. Breach of Confidentiality and Integrity	· Weak LAN encryption for network services can reveal user credentials to potential packet sniffing on the LAN, giving attackers access to IT systems and apps
	3. Weak Authentication	· Attackers can leverage repudiation and integrity verification weaknesses and in the case of email communications, interception of messages is possible leading to a breach in confidentiality and to a loss of trust
	4. Repudiation	· Weak authentication that can lead to potential impersonation and to unauthorized access of physical assets and resources.
	5. Network-Related Vulnerabilities	· Identity theft not put in check, leading to potential impersonation and to unauthorized access of logical and physical assets and resources.
Network Infrastructure	1. Unauthorized Access	· Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view LDAP credentials in cleartext
	2. Credential Harvesting	· Lack of NTAP can lead to traffic congestion and delays due to IDS working in real-time and not on duplicate/mirrored packets, which can potentially lead to loss of services availability.
	3. Network Congestion	· Deep Inspection Firewalls are already configured and cover all of this firewall's capabilities
	4. Poor IDS/IPS Performance	· Attackers can easily understand network topology and scan for vulnerable versions or Operating Systems using recon and scanning tools. Additionally they can perform DDoS attacks because ICMP echo requests are not disabled.
	5. Weak Protection against Recon and Scanning Tools	

Network Infrastructure Management	1. Unauthorized Access	· Attackers can easily understand network topology and scan for vulnerable versions or Operating Systems using recon and scanning tools. Additionally they can perform DDoS attacks because ICMP echo requests are not disabled.
	2. Credential Harvesting	· Attackers can abuse the lack of source IP check to spoof their source IP address to match the IP address of an internal device, leading to security compromises.
	3. IP Address Spoofing	· Since Cloudfare is deployed for DDoS mitigation, only internal attacks need to be mentioned - an attacker with internal network access or a compromised network node can perform SYN flood attacks leading to Denial of Service.
	4. ICMP Vulnerabilities	· Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view LDAP credentials in cleartext.
	5. SYN Flooding	· The DES key used for encryption in SNMPv2 can be cracked with enough time, leading to malicious network activity and network disruption.
Database	1. Weak Access Control	· Attackers can gain unauthorized access to DB which leads to a breach in confidentiality, and more potentially depending on the level of access the account they are using has.
	2. Unlimited Logon Attempts	· Keeping default account names makes it easier for attackers to guess the account name correctly and in turn makes it easier to brute-force the login.
	3. Uncapped TTL and Session Count	· Uncapped session TTL and count can lead to session hijacking attacks as well as denial of service attacks on the DB by flooding it with requests.
	4. Credential Harvesting	· Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view login credentials or other data in cleartext.
	5. No Load Balancing	· Lack of integrity check for the configuration files, data files and other files before DB startup can lead to malicious code execution and more.
Applications	1. Unauthorized Access	· Not clearing RAM or virtual memory can lead to code re-use attacks, or just data and code leakage in the case of a compromised system, which is a breach of confidentiality and help attackers in intel gathering.

	2. Credential Harvesting	· Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view login credentials or other data in cleartext.
	3. Breach of Confidentiality	· Attackers can gain unauthorized access to the app which leads to a breach in confidentiality, and more potentially depending on the level of access the account they compromise has.
	4. No Integrity Validation	· Attackers can potentially make unwanted and malicious changes to code leadings malicious code execution and more.
	5. Weak Authentication	· Not following best security practices when coding can lead to successful attacks against apps.
Wireless	1. Unauthorized Access	· Not using identity hiding which is one of the benefits of EAP-TTLS, so the authenticator is aware of both the username that establishes the TLS channel in the first phase and the user authenticated in the second phase
	2. Weak Authentication	· Attacker knows SSID of the router as it is discoverable, so he can perform different attacks and gain intel on the network's security posture. The attacker can also spoof access points SSID to trick guests.
	3. Weak Encryption	· Someone with physical access to a workstation that uses bluetooth can take advantage of some weak authentication methods.
	4. Network Device Publicly Discoverable	· Someone with access to an RFID tag can attempt to read data stored if it not well encrypted - passive RFID has weaker encryption than active RFID because the latter uses a battery.

Top 5 Vulnerability Risks across all categories

1. Unauthorized Access
2. Weak LAN Encryption
3. Uncapped TTL and Session Count
4. Credential Harvesting
5. IP Address Spoofing

Top 5 Asset Risks across all categories

1. Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view login credentials or other data in cleartext.

2. Keeping default account names makes it easier for attackers to guess the account name correctly and in turn makes it easier to brute-force the login.
3. Uncapped session TTL and count can lead to session hijacking attacks as well as denial of service attacks on the DB by flooding it with requests.
4. Attackers can easily understand network topology and scan for vulnerable versions or Operating Systems using recon and scanning tools. Additionally they can perform DDoS attacks because ICMP echo requests are not disabled.
5. Use of outdated network protocols can lead to successful network-related attacks, compromising integrity of the information systems as well as the confidentiality of data flowing across the network

10. Cybersecurity Workforce Risk Management Implementation

a. List of Cybersecurity Specialty Areas that exist in your company (see NCWF, Appendix A2)

Company Specialty Areas
Risk Management (RSK)
Software Development (DEV)
Systems Architecture (ARC)
Systems Requirements Planning (SRP)
Test and Evaluation (TST)
Systems Development (SYS)
Data Administration (DTA)
Customer Service and Technical Support (STS)
Network Services (NET)
Systems Administration (ADM)
Systems Analysis (ANA)
Legal Advice and Advocacy (LGA)
Training, Education, and Awareness (TEA)
Cybersecurity Management (MGT)
Strategic Planning and Policy (SPP)
Program/Project Management (PMA) and Acquisition
Cybersecurity Defense Analysis (CDA)
Incident Response (CIR)
Vulnerability Assessment and Management (VAM)
Threat Analysis (TWA)
All-Source Analysis (ASA)
Collection Operations (CLO)
Cyber Operational Planning (OPL)
Cyber Operations (OPS)
Digital Forensics (FOR)

b. List of Cybersecurity Work Roles that exist in your company (see NCWF, Appendix A3)

Company Work Roles

Authorizing Official/Designating Representative
Security Control Assessor
Software Developer
Secure Software Assessor
Enterprise Architect
Security Architect
Systems Requirements Planner
System Testing and Evaluation Specialist
Information Systems Security Developer
Systems Developer
Database Administrator
Data Analyst
Technical Support Specialist
Network Operations Specialist
System Administrator
Systems Security Analyst
Privacy Officer/Privacy Compliance Manager
Information Systems Security Manager
Cyber Policy and Strategy Planner
Program Manager
IT Project Manager
IT Program Auditor
Cyber Defense Analyst
Cyber Defense Incident Responder
Vulnerability Assessment Analyst
Threat/Warning Analyst
All-Source Analyst
All Source-Collection Manager
Cyber Ops Planner
Cyber Defense Forensics Analyst

c. List of Cybersecurity Tasks that exist in your company (see NCWF, Appendix A4)

Company Tasks
Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
Establish acceptable limits for the software application, network, or system.
Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.
Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.

Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.
Research current technology to understand capabilities of required system or network.
Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.
Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
Administer accounts, network rights, and access to systems and equipment.
Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).
Develop and implement network backup and recovery procedures.
Diagnose network connectivity problem.
Implement new system design procedures, test procedures, and quality standards.
Install or replace network hubs, routers, and switches.
Integrate new systems into existing network architecture.
Monitor network capacity and performance.
Patch network vulnerabilities to ensure that information is safeguarded against outside parties.
Provide feedback on network requirements, including network architecture and infrastructure.
Test and maintain network infrastructure including software and hardware devices.
Manage accounts, network rights, and access to systems and equipment.
Implement and enforce local network usage policies and procedures.
Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment.
Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information.
Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.
Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.
Develop contract language to ensure supply chain, system, network, and operational security are met.
Develop supply chain, system, network, performance, and cybersecurity requirements.
Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.
Conduct and/or support authorized penetration testing on enterprise network assets.
Apply and utilize authorized cyber capabilities to enable access to targeted networks.
Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access.
Monitor target networks to provide indications and warning of target communications changes or processing failures.
Produce network reconstructions.
Profile network or system administrators and their activities.
Conduct quality control to determine validity and relevance of information gathered about networks.
Generate and evaluate the effectiveness of network analysis strategies.

Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.)
Identify network components and their functionality to enable analysis and target development.
Reconstruct networks in diagram or report format.
Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.
Conduct access enabling of wireless computer and digital networks.
Conduct collection and processing of wireless computer and digital networks.
Conduct exploitation of wireless computer and digital networks.
Conduct network scouting and vulnerability analyses of systems within a network.
Conduct survey of computer and digital networks.
Detect exploits against targeted networks and hosts and react accordingly.
Exploit network devices, security devices, and/or terminals or environments using various methods or tools.
Facilitate access enabling by physical and/or wireless means.
Identify potential points of strength and vulnerability within a network.
Conduct cyber activities to degrade/remove information resident in computers and computer networks.
Fuse computer network attack analyses with criminal and counterintelligence investigations and operations.
Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.
Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.
Capture and analyze network traffic associated with malicious activities using network monitoring tools.
Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
Manage Accreditation Packages (e.g., ISO/IEC 15026-2).
Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).
Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
Verify and update security documentation reflecting the application/system security design features.
Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
Assess all the configuration management (change configuration/release management) processes.
Develop secure code and error handling.
Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.
Identify basic common coding flaws at a high level.

Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.
Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.
Perform integrated quality assurance testing for security functionality and resiliency attack.
Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.
Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language.
Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.
Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.
Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.
Identify and leverage the enterprise-wide version control system while designing and developing secure applications.
Consult with customers about software system design and maintenance.
Direct software programming and development of documentation.
Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.
Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.
Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate.
Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.
Develop software system testing and validation procedures, programming, and documentation.
Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.
Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.
Determine and document software patches or the extent of releases that would leave software vulnerable.
Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.
Apply secure code documentation.
Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.
Develop threat model based on customer interviews and requirements.

Consult with engineering staff to evaluate interface between hardware and software.
Perform penetration testing as required for new or updated applications.
Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application.
Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.
Develop secure software testing and validation procedures.
Develop system testing and validation procedures, programming, and documentation.
Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.
Employ secure configuration management processes.
Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.
Follow software and systems engineering life cycle standards and processes.
Oversee and make recommendations regarding configuration management.
Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware).
Create auditable evidence of security measures.
Analyze the results of software, hardware, or interoperability testing.
Perform developmental testing on systems under development.
Perform interoperability testing on systems exchanging electronic information with other systems.
Perform operational testing.
Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.
Develop and direct system testing and validation procedures and documentation.
Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.
Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable).
Employ configuration management processes.
Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations.
Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).
Maintain database management systems software.
Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.
Implement data mining and data warehousing applications.

Install and configure database management systems and software.
Conduct hypothesis testing using statistical processes.
Confer with systems analysts, engineers, programmers, and others to design application.
Troubleshoot system hardware and software.
Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.
Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.
Conduct functional and connectivity testing to ensure continuing operability.
Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.
Troubleshoot hardware/software interface and interoperability problems.
Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.
Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.
Implement specific cybersecurity countermeasures for systems and/or applications.
Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.
Perform cybersecurity testing of developed applications and/or systems.
Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.
Assess and monitor cybersecurity related to system implementation and testing practices.
Verify minimum security requirements are in place for all applications.
Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.
Review or conduct audits of information technology (IT) programs and projects.
Conduct import/export reviews for acquiring systems and software.
Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications.
Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.
Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s).
Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).
Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.

Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.
Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.
Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).
Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications.
Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.
Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.
Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.
Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.
Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).
Assess the effectiveness of security controls.
Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.
Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.
Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.
Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).
Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.
Identify and prioritize critical business functions in collaboration with organizational stakeholders.
Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
Conduct Privacy Impact Assessments (PIAs) of the application’s security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).

Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.
Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.
Design to security requirements to ensure requirements are met for all systems and/or applications.
Design hardware, operating systems, and software applications to adequately address requirements.
Analyze and plan for anticipated changes in data capacity requirements.
Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.
Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.
Manage the compilation, cataloging, caching, distribution, and retrieval of data.
Monitor and maintain databases to ensure optimal performance.
Perform backup and recovery of databases to ensure data integrity.
Provide recommendations on new database technologies and architectures.
Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems.
Maintain assured message delivery systems.
Implement data management standards, requirements, and specifications.
Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information.
Maintain incident tracking and solution database.
Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.
Assess adequate access controls based on principles of least privilege and need-to-know.
Ensure the execution of disaster recovery and continuity of operations.
Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.
Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.
Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements
Apply concepts, procedures, software, equipment, and/or technology applications to students.
Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).
Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.
Review, conduct, or participate in audits of cyber programs and projects.
Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.
Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.

Identify applications and operating systems of a network device based on network traffic.
Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).
Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).
Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).
Assist in the identification of intelligence collection shortfalls.
Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.
Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.
Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.
Support identification and documentation of collateral effects.
Perform foreign language and dialect identification in initial source data.
Determine existing collection management webpage databases, libraries and storehouses.
Identify potential collection disciplines for application against priority information requirements.
Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans.
Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.
Perform hash comparison against established database.
Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired.
Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.
Analyze candidate architectures, allocate security services, and select security mechanisms.
Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.
Analyze user needs and requirements to plan architecture.
Develop enterprise architecture or system components required to meet user needs.
Document and update as necessary all definition and architecture activities.

Assess the effectiveness of cybersecurity measures utilized by system(s).
Implement security designs for new or existing system(s).
Maintain baseline system security according to organizational policies.
Account for and administer individual requests for release or disclosure of personal and/or protected information
Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations
Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units
Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations
Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials
Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.
Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.
Recognize a possible security violation and take appropriate action to report the incident, as required.
Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
Coordinate with enterprise-wide cyber defense staff to validate network alerts.
Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.
Determine tactics, techniques, and procedures (TTPs) for intrusion sets.
Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).
Provide daily summary reports of network events and activity relevant to cyber defense practices.
Examine network topologies to understand data flows through the network.
Identify and analyze anomalies in network traffic using metadata.
Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.
Reconstruct a malicious attack or activity based off network traffic.
Identify network mapping and operating system (OS) fingerprinting activities.
Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave.

Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).
Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.
Conduct nodal analysis.
Apply analytic techniques to gain more target information.
Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers).
Develop new techniques for gaining and keeping access to target systems.
Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.

d. Comparison of the NCWF recommended Cybersecurity Specialty Areas with your company's existing Cybersecurity Specialty Areas

Recommended Specialty Areas	**Exists?**
Technology R&D (TRD)	No
Knowledge Management (KMG)	No
Executive Cyber Leadership (EXL)	No
Cybersecurity Defense Infrastructure Support (INF)	No
Exploitation Analysis (EXP)	No
Targets (TGT)	No
Language Analysis (LNG)	No
Cyber Investigation (INV)	No
Risk Management (RSK)	Yes
Software Development (DEV)	Yes
Systems Architecture (ARC)	Yes
Systems Requirements Planning (SRP)	Yes
Test and Evaluation (TST)	Yes
Systems Development (SYS)	Yes
Data Administration (DTA)	Yes
Customer Service and Technical Support (STS)	Yes
Network Services (NET)	Yes
Systems Administration (ADM)	Yes
Systems Analysis (ANA)	Yes
Legal Advice and Advocacy (LGA)	Yes
Training, Education, and Awareness (TEA)	Yes
Cybersecurity Management (MGT)	Yes
Strategic Planning and Policy (SPP)	Yes
Program/Project Management (PMA) and Acquisition	Yes
Cybersecurity Defense Analysis (CDA)	Yes
Incident Response (CIR)	Yes

Vulnerability Assessment and Management (VAM)	Yes
Threat Analysis (TWA)	Yes
All-Source Analysis (ASA)	Yes
Collection Operations (CLO)	Yes
Cyber Operational Planning (OPL)	Yes
Cyber Operations (OPS)	Yes
Digital Forensics (FOR)	Yes

e. Comparison of the NCWF recommended Cybersecurity Work Roles with your company's existing Cybersecurity Work Roles

Recommended Work Roles	**Exists?**
Research & Development Specialist	No
Knowledge Manager	No
Cyber Legal Advisor	No
Cyber Instructional Curriculum Developer	No
Cyber Instructor	No
Communications Security (COMSEC) Manager	No
Cyber Workforce Developer and Manager	No
Executive Cyber Leadership	No
Product Support Manager	No
IT Investment/Portfolio Manager	No
Cyber Defense Infrastructure Support Specialist	No
Exploitation Analyst	No
Mission Assessment Specialist	No
Target Developer	No
Target Network Analyst	No
Multi-Disciplined Language Analyst	No
All Source-Collection Requirements Manager	No
Cyber Intel Planner	No
Partner Integration Planner	No
Cyber Operator	No
Cyber Crime Investigator	No
Law Enforcement /CounterIntelligence Forensics Analyst	No
Authorizing Official/Designating Representative	Yes
Security Control Assessor	Yes
Software Developer	Yes
Secure Software Assessor	Yes
Enterprise Architect	Yes
Security Architect	Yes
Systems Requirements Planner	Yes

System Testing and Evaluation Specialist	Yes
Information Systems Security Developer	Yes
Systems Developer	Yes
Database Administrator	Yes
Data Analyst	Yes
Technical Support Specialist	Yes
Network Operations Specialist	Yes
System Administrator	Yes
Systems Security Analyst	Yes
Privacy Officer/Privacy Compliance Manager	Yes
Information Systems Security Manager	Yes
Cyber Policy and Strategy Planner	Yes
Program Manager	Yes
IT Project Manager	Yes
IT Program Auditor	Yes
Cyber Defense Analyst	Yes
Cyber Defense Incident Responder	Yes
Vulnerability Assessment Analyst	Yes
Threat/Warning Analyst	Yes
All-Source Analyst	Yes
All Source-Collection Manager	Yes
Cyber Ops Planner	Yes
Cyber Defense Forensics Analyst	Yes

f. Comparison the NCWF recommended Cybersecurity Tasks with your company's existing Cybersecurity Tasks

Recommended Tasks	**Exists?**
Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	No
Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.	No
Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	No
Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	No
Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.	No
Advocate organization's official position in legal and legislative proceedings.	No
Analyze and define data requirements and specifications.	No

Analyze and plan for anticipated changes in data capacity requirements.	Yes
Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.	Yes
Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.	Yes
Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.	No
Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.	No
Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	Yes
Apply secure code documentation.	Yes
Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Yes
Apply security policies to meet security objectives of the system.	No
Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.	No
Assess the effectiveness of cybersecurity measures utilized by system(s).	Yes
Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.	No
Develop content for cyber defense tools.	No
Build, test, and modify product prototypes using working models or theoretical models.	No
Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	Yes
Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	Yes
Collect and maintain data needed to meet system cybersecurity reporting.	No
Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	No
Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.	No
Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.	Yes
Conduct and/or support authorized penetration testing on enterprise network assets.	Yes
Conduct functional and connectivity testing to ensure continuing operability.	Yes
Conduct interactive training exercises to create an effective learning environment.	No
Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.	No

Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Yes
Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications.	No
Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.	No
Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).	Yes
Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.	Yes
Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users.	No
Develop threat model based on customer interviews and requirements.	Yes
Consult with customers to evaluate functional requirements.	No
Consult with engineering staff to evaluate interface between hardware and software.	Yes
Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.	No
Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications.	Yes
Coordinate with enterprise-wide cyber defense staff to validate network alerts.	Yes
Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	No
Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions.	No
Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.	No
Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.	No
Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats.	No
Decrypt seized data using technical means.	No
Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	Yes

Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	No
Define project scope and objectives based on customer requirements.	No
Design and develop cybersecurity or cybersecurity-enabled products.	No
Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	Yes
Design hardware, operating systems, and software applications to adequately address cybersecurity requirements.	No
Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.	Yes
Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.	No
Determine level of assurance of developed capabilities based on test results.	No
Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.	No
Develop an understanding of the needs and requirements of information end-users.	No
Develop and direct system testing and validation procedures and documentation.	Yes
Develop and document requirements, capabilities, and constraints for design procedures and processes.	No
Develop and document systems administration standard operating procedures.	No
Review and validate data mining and data warehousing programs, processes, and requirements.	No
Develop and implement network backup and recovery procedures.	Yes
Develop and maintain strategic plans.	No
Develop architectures or system components consistent with technical specifications.	No
Develop data standards, policies, and procedures.	No
Develop detailed security design documentation for component and interface specifications to support system design and development.	No
Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.	Yes

Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).	No
Develop methods to monitor and measure risk, compliance, and assurance efforts.	No
Develop new or identify existing awareness and training materials that are appropriate for intended audiences.	No
Develop policy, programs, and guidelines for implementation.	No
Provide technical summary of findings in accordance with established reporting procedures.	No
Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.	No
Develop secure code and error handling.	Yes
Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications.	No
Develop specifications to ensure that risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level.	No
Develop test plans to address specifications and requirements.	No
Diagnose network connectivity problem.	Yes
Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.	Yes
Draft statements of preliminary or residual security risks for system operation.	No
Employ secure configuration management processes.	Yes
Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	No
Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.	Yes
Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.	No
Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	No
Ensure that security improvement actions are evaluated, validated, and implemented as required.	No

Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.	No
Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment.	Yes
Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).	No
Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture.	No
Establish and maintain communication channels with stakeholders.	No
Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy.	No
Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).	No
Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.	No
Evaluate contracts to ensure compliance with funding, legal, and program requirements.	No
Evaluate cost/benefit, economic, and risk analysis in decision-making process.	No
Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	Yes
Evaluate the effectiveness and comprehensiveness of existing training programs.	No
Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.	No
Examine recovered data for information of relevance to the issue at hand.	No
Fuse computer network attack analyses with criminal and counterintelligence investigations and operations.	Yes
Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements.	No
Identify alternative information security strategies to address organizational security objective.	No
Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable).	Yes
Identify and prioritize critical business functions in collaboration with organizational stakeholders.	Yes
Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.	No

Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.	No
Identify basic common coding flaws at a high level.	Yes
Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.	No
Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	No
Identify elements of proof of the crime.	No
Identify information technology (IT) security program implications of new technologies or technology upgrades.	No
Identify organizational policy stakeholders.	No
Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.	Yes
Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.	Yes
Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization's evaluation and validation requirements.	No
Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.	Yes
Implement new system design procedures, test procedures, and quality standards.	Yes
Implement security designs for new or existing system(s).	Yes
Implement specific cybersecurity countermeasures for systems and/or applications.	Yes
Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).	No
Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Yes
Install or replace network hubs, routers, and switches.	Yes
Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements.	No
Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.	No
Integrate new systems into existing network architecture.	Yes

Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information.	Yes
Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.	No
Interpret and/or approve security requirements relative to the capabilities of new information technologies.	No
Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	No
Lead and align information technology (IT) security priorities with the security strategy.	No
Lead and oversee information security budget, staffing, and contracting.	No
Maintain baseline system security according to organizational policies.	Yes
Maintain database management systems software.	Yes
Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.	Yes
Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.	Yes
Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.	Yes
Maintain information systems assurance and accreditation materials.	No
Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.	Yes
Make recommendations based on test results.	No
Manage accounts, network rights, and access to systems and equipment.	Yes
Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).	Yes
Manage the compilation, cataloging, caching, distribution, and retrieval of data.	Yes
Manage the monitoring of information security data sources to maintain organizational situational awareness.	No
Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.	Yes
Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.	No

Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements.	No
Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.	No
Monitor and maintain databases to ensure optimal performance.	Yes
Monitor network capacity and performance.	Yes
Monitor and report the usage of knowledge management assets and resources.	No
Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.	No
Oversee and make recommendations regarding configuration management.	Yes
Oversee the information security training and awareness program.	No
Participate in an information security risk assessment during the Security Assessment and Authorization process.	No
Participate in the development or modification of the computer environment cybersecurity program plans and requirements.	No
Patch network vulnerabilities to ensure that information is safeguarded against outside parties.	Yes
Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.	Yes
Perform backup and recovery of databases to ensure data integrity.	Yes
Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.	No
Perform cyber defense trend analysis and reporting.	No
Perform dynamic analysis to boot an "image" of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment.	No
Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.	No
Perform file signature analysis.	No
Perform hash comparison against established database.	Yes
Perform cybersecurity testing of developed applications and/or systems.	Yes

Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.	No
Perform integrated quality assurance testing for security functionality and resiliency attack.	Yes
Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).	No
Perform timeline analysis.	No
Perform needs analysis to determine opportunities for new and improved business process solutions.	No
Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).	Yes
Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.	Yes
Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Yes
Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.	Yes
Perform static media analysis.	No
Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.	Yes
Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Yes
Perform tier 1, 2, and 3 malware analysis.	No
Perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks.	No
Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.	Yes
Plan and manage the delivery of knowledge management projects.	No
Plan, execute, and verify data redundancy and system recovery procedures.	No
Plan and recommend modifications or adjustments based on exercise results or system environment.	No
Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.	Yes
Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language.	Yes
Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).	No
Prepare use cases to justify the need for specific information technology (IT) solutions.	No

Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.	Yes
Process crime scenes.	No
Properly document all systems security implementation, operations, and maintenance activities and update as necessary.	No
Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements.	No
Provide advice on project costs, design concepts, or design changes.	No
Provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant cybersecurity compliances.	No
Provide daily summary reports of network events and activity relevant to cyber defense practices.	Yes
Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	No
Provide feedback on network requirements, including network architecture and infrastructure.	Yes
Provide guidelines for implementing developed systems to customers or installation teams.	No
Provide cybersecurity guidance to leadership.	No
Provide input on security requirements to be included in statements of work and other appropriate procurement documents.	No
Provide input to implementation plans and standard operating procedures.	No
Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Yes
Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.	No
Provide ongoing optimization and problem-solving support.	No
Provide recommendations for possible improvements and upgrades.	No
Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information.	Yes
Provide recommendations on new database technologies and architectures.	Yes
Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.	No
Provide technical assistance on digital evidence matters to appropriate personnel.	No

Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.	No
Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Yes
Recognize a possible security violation and take appropriate action to report the incident, as required.	Yes
Recognize and accurately report forensic artifacts indicative of a particular operating system.	No
Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	Yes
Recommend new or revised security, resilience, and dependability measures based on the results of reviews.	No
Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.	No
Resolve conflicts in laws, regulations, policies, standards, or procedures.	No
Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Yes
Review existing and proposed policies with stakeholders.	No
Review or conduct audits of information technology (IT) programs and projects.	Yes
Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions).	No
Secure the electronic device or information source.	No
Serve on agency and interagency policy boards.	No
Recommend policy and coordinate review and approval.	No
Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Yes
Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	No
Support the design and execution of exercise scenarios.	No
Provide support to security/certification test and evaluation activities.	No
Test and maintain network infrastructure including software and hardware devices.	Yes
Track and document cyber defense incidents from initial detection through final resolution.	No
Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.	Yes
Translate functional requirements into technical solutions.	No
Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.	Yes

Troubleshoot system hardware and software.	Yes
Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).	No
Use federal and organization-specific published documents to manage operations of their computing environment system(s).	No
Capture and analyze network traffic associated with malicious activities using network monitoring tools.	Yes
Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	No
Utilize models and simulations to analyze or predict system performance under different operating conditions.	No
Verify and update security documentation reflecting the application/system security design features.	Yes
Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.	Yes
Verify that the software application/network/system accreditation and assurance documentation is current.	No
Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.	No
Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.	No
Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	No
Research current technology to understand capabilities of required system or network.	Yes
Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.	Yes
Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).	Yes
Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).	Yes
Conduct cursory binary analysis.	No
Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.	No
Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.	No
Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	No
Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated.	No

Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.	Yes
Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.	Yes
Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.	No
Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.	No
Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).	Yes
Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.	No
Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Yes
Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.	Yes
Perform penetration testing as required for new or updated applications.	Yes
Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.	Yes
Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.	Yes
Design and develop key management functions (as related to cybersecurity).	No
Analyze user needs and requirements to plan and conduct system security development.	No
Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).	No
Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.	Yes
Develop and document supply chain risks for critical system elements, as appropriate.	No
Create auditable evidence of security measures.	Yes
Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).	Yes
Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.	No
Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	No

Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	Yes
Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.	No
Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.	Yes
Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary.	No
Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Yes
Collaborate with stakeholders to identify and/or develop appropriate solutions technology.	No
Design and develop new tools/technologies as related to cybersecurity.	No
Perform virus scanning on digital media.	No
Perform file system forensic analysis.	No
Perform static analysis to mount an "image" of a drive (without necessarily having the original drive).	No
Perform static malware analysis.	No
Utilize deployable forensics toolkit to support operations as necessary.	No
Determine tactics, techniques, and procedures (TTPs) for intrusion sets.	Yes
Examine network topologies to understand data flows through the network.	Yes
Recommend computing environment vulnerability corrections.	No
Identify and analyze anomalies in network traffic using metadata.	Yes
Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).	No
Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.	Yes
Isolate and remove malware.	No
Identify applications and operating systems of a network device based on network traffic.	Yes
Reconstruct a malicious attack or activity based off network traffic.	Yes
Identify network mapping and operating system (OS) fingerprinting activities.	Yes
Develop and document User Experience (UX) requirements including information architecture and user interface requirements.	No
Develop and implement cybersecurity independent audit processes for application software/networks/systems and oversee ongoing independent audits to ensure that operational and Research and Design (R&D) processes and procedures are in compliance with organizational and mandatory cybersecurity requirements and accurately followed by Systems Administrators and other cybersecurity staff when performing their day-to-day activities.	No
Develop contract language to ensure supply chain, system, network, and operational security are met.	Yes

Identify and leverage the enterprise-wide version control system while designing and developing secure applications.	Yes
Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.	No
Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.	Yes
Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems.	Yes
Analyze candidate architectures, allocate security services, and select security mechanisms.	Yes
Analyze incident data for emerging trends.	No
Assess the effectiveness of security controls.	Yes
Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave.	Yes
Consult with customers about software system design and maintenance.	Yes
Coordinate with intelligence analysts to correlate threat assessment data.	No
Design and document quality standards.	No
Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.	Yes
Develop and deliver technical training to educate others or meet customer needs.	No
Develop or assist in the development of computer based training modules or classes.	No
Develop or assist in the development of course assignments.	No
Develop or assist in the development of course evaluations.	No
Develop or assist in the development of grading and proficiency standards.	No
Assist in the development of individual/collective development, training, and/or remediation plans.	No
Develop or assist in the development of learning objectives and goals.	No
Develop or assist in the development of on-the-job training materials or programs.	No
Develop or assist in the development of written tests for measuring and assessing learner proficiency.	No
Direct software programming and development of documentation.	Yes
Document a system's purpose and preliminary system security concept of operations.	No
Employ configuration management processes.	Yes
Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.	Yes
Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.	No
Follow software and systems engineering life cycle standards and processes.	Yes
Maintain assured message delivery systems.	Yes
Maintain incident tracking and solution database.	Yes

Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.	No
Perform cyber defense trend analysis and reporting.	No
Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware).	Yes
Build, install, configure, and test dedicated cyber defense hardware.	No
WITHDRAWN: Integrated with T0228	No
Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.	Yes
Write detailed functional specifications that document the architecture development process.	No
Lead efforts to promote the organization's use of knowledge management and information sharing.	No
Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	No
Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	No
Analyze data sources to provide actionable recommendations.	No
Analyze the crisis to ensure public, personal, and resource protection.	No
Assess all the configuration management (change configuration/release management) processes.	Yes
Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction.	No
Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation.	No
Assess the validity of source data and subsequent findings.	No
Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.	No
Collect metrics and trending data.	No
Conduct a market analysis to identify, assess, and recommend commercial, Government off-the-shelf, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements.	No
Conduct hypothesis testing using statistical processes.	Yes
Conduct learning needs assessments and identify requirements.	No
Confer with systems analysts, engineers, programmers, and others to design application.	Yes
Coordinate and manage the overall service provided to a customer end-to-end.	No
Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.	No

Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.	No
Create interactive learning exercises to create an effective learning environment.	No
Design and develop system administration and management functionality for privileged access users.	No
Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.	No
Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks.	No
Develop and facilitate data-gathering methods.	No
Develop and implement standardized position descriptions based on established cyber work roles.	No
Develop and review recruiting, hiring, and retention procedures in accordance with current HR policies.	No
Develop cyber career field classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers.	No
Develop or assist in the development of training policies and protocols for cyber training.	No
Develop strategic insights from large data sets.	No
Develop the goals and objectives for cyber curriculum.	No
Ensure that cyber career fields are managed in accordance with organizational HR policies and directives.	No
Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.	No
Ensure that appropriate Service-Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service.	No
Establish acceptable limits for the software application, network, or system.	Yes
Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.	No
Establish and oversee waiver processes for cyber career field entry and training qualification requirements.	No
Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.	No
Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.	No
Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements.	No
Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	No

Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle).	No
Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).	No
Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers.	No
Present technical information to technical and nontechnical audiences.	No
Present data in creative formats.	No
Program custom algorithms.	No
Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	No
Provide actionable recommendations to critical stakeholders based on data analysis and findings.	No
Provide criminal investigative support to trial counsel during the judicial process.	No
Review and apply cyber career field qualification standards.	No
Review and apply organizational policies related to or influencing the cyber workforce.	No
Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	No
Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	No
Support integration of qualified cyber workforce personnel into information systems life cycle development processes.	No
Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method.	No
Validate specifications and requirements for testability.	No
Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.	No
Write and publish after action reviews.	No
Process image with appropriate tools depending on analyst’s goals.	No
Perform Windows registry analysis.	No
Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.	No
Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired.	Yes
Correlate incident data and perform cyber defense reporting.	No
Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.	Yes
Effectively allocate storage capacity in the design of data management systems.	No

Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).	No
Utilize different programming languages to write code, open files, read files, and write output to different files.	No
Utilize open source language such as R and apply quantitative techniques (e.g., descriptive and inferential statistics, sampling, experimental design, parametric and non-parametric tests of difference, ordinary least squares regression, general line).	No
Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.	No
Participate in the acquisition process as necessary.	No
Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	No
Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases.	No
Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities.	No
Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.	No
Conduct import/export reviews for acquiring systems and software.	Yes
Develop data management capabilities (e.g., cloud-based, centralized cryptographic key management) to include support to the mobile workforce.	No
Develop supply chain, system, network, performance, and cybersecurity requirements.	Yes
Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Yes
Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.	Yes
Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate.	Yes
Install, update, and troubleshoot systems/servers.	No
Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.	No
Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s).	Yes
Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files).	No
Implement data management standards, requirements, and specifications.	Yes
Analyze computer-generated threats for counter intelligence or criminal activity.	No

Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application.	Yes
Analyze organizational cyber policy.	No
Analyze the results of software, hardware, or interoperability testing.	Yes
Analyze user needs and requirements to plan architecture.	Yes
Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.	Yes
Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	No
Gather and preserve evidence used on the prosecution of computer crimes.	No
Check system hardware availability, functionality, integrity, and efficiency.	No
Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	No
Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.	Yes
Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance.	No
Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.	Yes
Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.	Yes
Correlate training and learning to business or mission requirements.	No
Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).	Yes
Detect and analyze encrypted data, stenography, alternate data streams and other forms of concealed data.	No
Capture and integrate essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	No
Define and integrate current and future mission environments.	No
Create training courses tailored to the audience and physical environment.	No
Deliver training courses tailored to the audience and physical/virtual environments.	No
Apply concepts, procedures, software, equipment, and/or technology applications to students.	Yes
Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan.	No
Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.	Yes
Design hardware, operating systems, and software applications to adequately address requirements.	Yes
Develop enterprise architecture or system components required to meet user needs.	Yes

Design to security requirements to ensure requirements are met for all systems and/or applications.	Yes
Design training curriculum and course content based on requirements.	No
Participate in development of training curriculum and course content.	No
Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization's intellectual capital.	No
Determine and develop leads and identify sources of information to identify and/or prosecute the responsible parties to an intrusion or other crimes.	No
Define baseline security requirements in accordance with applicable guidelines.	No
Develop software system testing and validation procedures, programming, and documentation.	Yes
Develop secure software testing and validation procedures.	Yes
Develop system testing and validation procedures, programming, and documentation.	Yes
Comply with organization systems administration standard operating procedures.	No
Implement data mining and data warehousing applications.	Yes
Develop and implement data mining and data warehousing programs.	No
Implement and enforce local network usage policies and procedures.	Yes
Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements.	No
Develop cost estimates for new or modified system(s).	No
Develop detailed design documentation for component and interface specifications to support system design and development.	No
Develop guidelines for implementation.	No
Develop mitigation strategies to address cost, schedule, performance, and security risks.	No
Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness.	No
Diagnose and resolve customer reported system incidents, problems, and events.	No
Analyze and report organizational security posture trends.	No
Analyze and report system security posture trends.	No
Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).	No
Draft, staff, and publish cyber policy.	No
Document and update as necessary all definition and architecture activities.	Yes
Provide legal analysis and decisions to inspectors general, privacy officers, oversight and compliance personnel regarding compliance with cybersecurity policies and relevant legal and regulatory requirements.	No
Assess adequate access controls based on principles of least privilege and need-to-know.	Yes
Evaluate the impact of changes to laws, regulations, policies, standards, or procedures.	No
Ensure the execution of disaster recovery and continuity of operations.	Yes
Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.	No

Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property.	No
Identify components or elements, allocate comprehensive functional components to include security functions, and describe the relationships between the elements.	No
Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Yes
Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.	Yes
Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).	Yes
Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.	Yes
Implement security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed.	No
Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.	No
Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures.	No
Implement designs for new or existing system(s).	No
Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.	Yes
Install and configure database management systems and software.	Yes
Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.	Yes
Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment.	No
Lead and oversee budget, staffing, and contracting.	No
Administer accounts, network rights, and access to systems and equipment.	Yes
Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	Yes
Perform asset management/inventory of information technology (IT) resources.	No
Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements.	No
Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	No
Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.	Yes
Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.	Yes
Monitor and maintain system/server configuration.	No
Monitor and report client-level computer system performance.	No

Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.	Yes
Assess and monitor cybersecurity related to system implementation and testing practices.	Yes
Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Yes
Seek consensus on proposed policy changes from stakeholders.	No
Oversee installation, implementation, configuration, and support of system components.	No
Verify minimum security requirements are in place for all applications.	Yes
Perform an information security risk assessment.	No
Coordinate incident response functions.	No
Perform developmental testing on systems under development.	Yes
Perform interoperability testing on systems exchanging electronic information with other systems.	Yes
Perform operational testing.	Yes
Diagnose faulty system/server hardware.	No
Perform repairs on faulty system/server hardware.	No
Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.	Yes
Integrate results regarding the identification of gaps in security architecture.	No
Perform security reviews and identify security gaps in architecture.	No
Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for the most effective learning environment.	No
Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses).	No
Plan implementation strategy to ensure that enterprise components can be integrated and aligned.	No
Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).	No
Prepare reports to document the investigation following legal standards and requirements.	No
Promote knowledge sharing between information owners/users through an organization's operational processes and systems.	No
Provide enterprise cybersecurity and supply chain risk management guidance.	No
Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	No
Provide input to implementation plans and standard operating procedures as they relate to information systems security.	No
Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials	No
Provide policy guidance to cyber management, staff, and users.	No

Develop a trend analysis and impact report.	No
Troubleshoot hardware/software interface and interoperability problems.	Yes
Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.	No
Review, conduct, or participate in audits of cyber programs and projects.	Yes
Conduct periodic reviews/revisions of course content for accuracy, completeness alignment, and currency (e.g., course content documents, lesson plans, student texts, examinations, schedules of instruction, and course descriptions).	No
Recommend revisions to curriculum and course content based on feedback from previous training sessions.	No
Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	No
Support the CIO in the formulation of cyber-related policies.	No
Provide support to test and evaluation activities.	No
Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.	Yes
Record and manage test data.	No
Trace system requirements to design components and perform gap analysis.	No
Translate proposed capabilities into technical requirements.	No
WITHDRAWN: Use data carving techniques (e.g., FTK-Foremost) to extract data for further analysis.	No
Verify stability, interoperability, portability, and/or scalability of system architecture.	No
Work with stakeholders to resolve computer security incidents and vulnerability compliance.	No
Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.	No
Research and evaluate available technologies and standards to meet customer requirements.	No
Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	Yes
Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).	No
Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).	Yes
Draft and publish supply chain security and risk management documents.	No
Review and approve a supply chain security/risk management policy.	No
Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	Yes
Determine and document software patches or the extent of releases that would leave software vulnerable.	Yes

Document how the implementation of a new system or new interface between systems impacts the current and target environment including but not limited to security posture.	No
Assess and design security management functions as related to cyberspace.	No
Integrate key management functions as related to cyberspace.	No
Analyze user needs and requirements to plan and conduct system development.	No
Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations.	Yes
Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).	No
Accurately characterize targets.	No
Adjust collection operations or collection plan to address identified issues/challenges and to synchronize collections with overall operational requirements.	No
Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives.	No
Analyze feedback to determine extent to which collection products and services are meeting requirements.	No
Analyze incoming collection requests.	No
Analyze internal operational architecture, tools, and procedures for ways to improve performance.	No
Analyze target operational architecture for ways to gain access.	No
Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and requirement s (e.g., duration, scope, communication requirements, interagency/international agreements).	No
Answer requests for information.	No
Apply and utilize authorized cyber capabilities to enable access to targeted networks.	Yes
Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement.	No
Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements.	No
Assess and apply operational environment factors and risks to collection management process.	No
Apply and obey applicable statutes, laws, regulations and policies.	No
Coordinate for intelligence support to operational planning activities.	No
Assess all-source intelligence and recommend targets to support cyber operation objectives.	No
Assess efficiency of existing information exchange and management systems.	No
Assess performance of collection assets against prescribed specifications.	No
Assess target vulnerabilities and/or operational capabilities to determine course of action.	No

Assess the effectiveness of collections in satisfying priority information gaps, using available capabilities and methods, and adjust collection strategies and collection requirements accordingly.	No
Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.	No
Provide expertise to course of action development.	No
Provide subject matter expertise to the development of a common operational picture.	No
Maintain a common intelligence picture.	No
Provide subject matter expertise to the development of cyber operations specific indicators.	No
Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	No
Assist in the development and refinement of priority information requirements.	No
Provide expertise to the development of measures of effectiveness and measures of performance.	No
Assist in the identification of intelligence collection shortfalls.	Yes
Enable synchronization of intelligence support plans across partner organizations as required.	No
Perform analysis for target infrastructure exploitation activities.	No
Provide input to the identification of cyber-related success criteria.	No
Brief threat and/or target current situations.	No
Build and maintain electronic target folders.	No
Classify documents in accordance with classification guidelines.	No
Close requests for information once satisfied.	No
Collaborate with intelligence analysts/targeting organizations involved in related areas.	No
Collaborate with development organizations to create and deploy the tools needed to achieve objectives.	No
Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.	No
Collaborate with other internal and external partner organizations on target access and operational issues.	No
Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials).	No
Collaborate with customer to define information requirements.	No
Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers.	No
Compare allocated and available assets to collection demand as expressed through requirements.	No
Compile lessons learned from collection management activity's execution of organization collection objectives.	No
Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.	No

Identify and conduct analysis of target communications to identify information essential to support operations.	No
Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access.	Yes
Conduct access enabling of wireless computer and digital networks.	Yes
Conduct collection and processing of wireless computer and digital networks.	Yes
Conduct end-of-operations assessments.	No
Conduct exploitation of wireless computer and digital networks.	Yes
Conduct formal and informal coordination of collection requirements in accordance with established guidelines and procedures.	No
Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access.	No
Conduct in-depth research and analysis.	No
Conduct network scouting and vulnerability analyses of systems within a network.	Yes
Conduct nodal analysis.	Yes
Conduct on-net activities to control and exfiltrate data from deployed technologies.	No
Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies.	No
Conduct open source data collection via various online tools.	No
Conduct quality control to determine validity and relevance of information gathered about networks.	Yes
Develop, review and implement all levels of planning guidance in support of cyber operations.	No
Conduct survey of computer and digital networks.	Yes
Conduct target research and analysis.	No
Consider efficiency and effectiveness of collection assets and resources if/when applied against priority information requirements.	No
Construct collection plans and matrixes using established guidance and procedures.	No
Contribute to crisis action planning for cyber operations.	No
Contribute to the development of the organization's decision support tools if necessary.	No
Contribute to the development, staffing, and coordination of cyber operations policies, performance standards, plans and approval packages with appropriate internal and/or external decision makers.	No
Incorporate intelligence equities into the overall design of cyber operations plans.	No
Coordinate resource allocation of collection assets against prioritized collection requirements with collection discipline leads.	No
Coordinate inclusion of collection plan in appropriate documentation.	No
Coordinate target vetting with appropriate partners.	No
Re-task or re-direct collection assets and resources.	No
Coordinate with intelligence and cyber defense partners to obtain relevant essential information.	No

Coordinate with intelligence planners to ensure that collection managers receive information requirements.	No
Coordinate with the intelligence planning team to assess capability to satisfy assigned intelligence tasks.	No
Coordinate, produce, and track intelligence requirements.	No
Coordinate, synchronize and draft applicable intelligence sections of cyber operations plans.	No
Use intelligence estimates to counter potential target actions.	No
Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities.	No
Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.	No
Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers).	Yes
Detect exploits against targeted networks and hosts and react accordingly.	Yes
Determine course of action for addressing changes to objectives, guidance, and operational environment.	No
Determine existing collection management webpage databases, libraries and storehouses.	Yes
Determine how identified factors affect the tasking, collection, processing, exploitation and dissemination architecture's form and function.	No
Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives.	No
Determine organizations and/or echelons with collection authority over all accessible collection assets.	No
Determine what technologies are used by a given target.	No
Develop a method for comparing collection reports to outstanding requirements to identify information gaps.	No
Develop all-source intelligence targeting materials.	No
Apply analytic techniques to gain more target information.	Yes
Develop and maintain deliberate and/or crisis plans.	No
Develop and review specific cyber operations guidance for integration into broader planning activities.	No
Develop and review intelligence guidance for integration into supporting cyber operations planning and execution.	No
Develop coordinating instructions by collection discipline for each phase of an operation.	No
Develop cyber operations plans and guidance to ensure that execution and resource allocation decisions align with organization objectives.	No
Develop detailed intelligence support to cyber operations requirements.	No
Develop information requirements necessary for answering priority information requests.	No
Develop measures of effectiveness and measures of performance.	No
Allocate collection assets based on leadership's guidance, priorities, and/or operational emphasis.	No
Develop munitions effectiveness assessment or operational assessment materials.	No

Develop new techniques for gaining and keeping access to target systems.	Yes
Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations.	No
Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives.	No
Develop potential courses of action.	No
Develop procedures for providing feedback to collection managers, asset managers, and processing, exploitation and dissemination centers.	No
Develop strategy and processes for partner planning, operations, and capability development.	No
Develop, implement, and recommend changes to appropriate planning procedures and policies.	No
Develop, maintain, and assess cyber cooperation security agreements with external partners.	No
Devise, document, and validate cyber operation strategy and planning documents.	No
Disseminate reports to inform decision makers on collection issues.	No
Disseminate tasking messages and collection plans.	No
Conduct and document an assessment of the collection results using established procedures.	No
Draft cyber intelligence collection and production requirements.	No
Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems.	No
Engage customers to understand customers' intelligence needs and wants.	No
Ensure operational planning efforts are effectively transitioned to current operations.	No
Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines.	No
Establish alternative processing, exploitation and dissemination pathways to address identified issues or problems.	No
Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership.	No
Establish processing, exploitation and dissemination management activity using approved guidance and/or procedures.	No
Estimate operational effects generated through cyber activities.	No
Evaluate threat decision-making processes.	No
Identify threat vulnerabilities.	No
Identify threats to Blue Force vulnerabilities.	No
Evaluate available capabilities against desired effects to recommend efficient solutions.	No
Evaluate extent to which collected information and/or produced intelligence satisfy information requests.	No
Evaluate intelligence estimates to support the planning cycle.	No
Evaluate the conditions that affect employment of available cyber intelligence capabilities.	No
Generate and evaluate the effectiveness of network analysis strategies.	Yes

Evaluate extent to which collection operations are synchronized with operational requirements.	No
Evaluate the effectiveness of collection operations against the collection plan.	No
Examine intercept-related metadata and content with an understanding of targeting significance.	No
Exploit network devices, security devices, and/or terminals or environments using various methods or tools.	Yes
Facilitate access enabling by physical and/or wireless means.	Yes
Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers.	No
Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.	No
Facilitate the sharing of “best practices” and “lessons learned” throughout the cyber operations community.	No
Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development.	No
Formulate collection strategies based on knowledge of available intelligence discipline capabilities and gathering methods that align multi-discipline collection capabilities and accesses with targets and their observables.	No
Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities.	No
Incorporate cyber operations and communications security support plans into organization objectives.	No
Incorporate intelligence and counterintelligence to support plan development.	No
Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.)	Yes
Generate requests for information.	No
Identify threat tactics, and methodologies.	No
Identify all available partner intelligence capabilities and limitations supporting cyber operations.	No
Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	No
Identify, draft, evaluate, and prioritize relevant intelligence or information requirements.	No
Identify and manage security cooperation priorities with external partners.	No
Identify and submit intelligence requirements for the purposes of designating priority information requirements.	No
Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.	No
Identify collection gaps and potential collection strategies against targets.	No
Identify coordination requirements and procedures with designated collection authorities.	No
Identify critical target elements.	No
Identify intelligence gaps and shortfalls.	No

Identify cyber intelligence gaps and shortfalls for cyber operational planning.	No
Identify gaps in our understanding of target technology and developing innovative collection approaches.	No
Identify issues or problems that can disrupt and/or degrade processing, exploitation and dissemination architecture effectiveness.	No
Identify network components and their functionality to enable analysis and target development.	Yes
Identify potential collection disciplines for application against priority information requirements.	Yes
Identify potential points of strength and vulnerability within a network.	Yes
Identify and mitigate risks to collection management ability to support the plan, operations and target cycle.	No
Identify the need, scope, and timeframe for applicable intelligence environment preparation derived production.	No
Identify, locate, and track targets via geospatial analysis techniques.	No
Provide input to or develop courses of action based on threat factors.	No
Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities.	No
Inform stakeholders (e.g., collection managers, asset managers, processing, exploitation and dissemination centers) of evaluation results using established procedures.	No
Initiate requests to guide tasking and assist with collection management.	No
Integrate cyber planning/targeting efforts with other organizations.	No
Interpret environment preparations assessments to determine a course of action.	No
Issue requests for information.	No
Lead and coordinate intelligence support to operational planning.	No
Lead or enable exploitation operations in support of organization objectives and target requirements.	No
Link priority collection requirements to optimal assets and resources.	No
Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications.	Yes
Maintain relationships with internal and external partners involved in cyber planning or related areas.	No
Maintain situational awareness and functionality of organic operational infrastructure.	No
Maintain situational awareness of cyber-related intelligence requirements and associated tasking.	No
Maintain situational awareness of partner capabilities and activities.	No
Maintain situational awareness to determine if changes to the operating environment require review of the plan.	No
Maintain target lists (i.e., RTL, JTL, CTL, etc.).	No
Make recommendations to guide collection in support of customer requirements.	No
Modify collection requirements as necessary.	No

Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.	No
Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	No
Monitor and report on validated threat activities.	No
Monitor completion of reallocated collection efforts.	No
Monitor open source websites for hostile content directed towards organizational or partner interests.	No
Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.	No
Monitor operational status and effectiveness of the processing, exploitation and dissemination architecture.	No
Monitor target networks to provide indications and warning of target communications changes or processing failures.	Yes
Monitor the operational environment for potential factors and risks to the collection operation management process.	No
Operate and maintain automated systems for gaining and maintaining access to target systems.	No
Optimize mix of collection assets and resources to increase effectiveness and efficiency against essential information associated with priority intelligence requirements.	No
Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	No
Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy.	No
Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.	No
Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Yes
WITHDRAWN: Provide subject matter expertise in course of action development.	No
Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Yes
Provide subject matter expertise to planning efforts with internal and external cyber operations partners.	No
Provide subject matter expertise to development of exercises.	No
Propose policy which governs interactions with external coordination groups.	No
Perform content and/or metadata analysis to meet organization objectives.	No
Conduct cyber activities to degrade/remove information resident in computers and computer networks.	Yes
Perform targeting automation activities.	No
Characterize websites.	No

Provide subject matter expertise to website characterizations.	No
Prepare for and provide subject matter expertise to exercises.	No
Prioritize collection requirements for collection platforms based on platform capabilities.	No
Process exfiltrated data for analysis and/or dissemination to customers.	No
Produce network reconstructions.	Yes
Produce target system analysis products.	No
Profile network or system administrators and their activities.	Yes
Profile targets and their activities.	No
Provide advice/assistance to operations and intelligence decision makers with reassignment of collection assets and resources in response to dynamic operational situations.	No
Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans.	Yes
Provide aim point and reengagement recommendations.	No
Provide analyses and support for effectiveness assessment.	No
Provide current intelligence support to critical internal/external stakeholders as appropriate.	No
Provide cyber focused guidance and advice on intelligence support plan inputs.	No
Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	No
Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.	Yes
Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.	No
Provide input and assist in post-action effectiveness assessments.	No
Provide input and assist in the development of plans and guidance.	No
Provide input for targeting effectiveness assessments for leadership acceptance.	No
Provide input to the administrative and logistical elements of an operational support plan.	No
Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.	Yes
Provide effectiveness support to designated exercises, and/or time sensitive operations.	No
Provide operations and reengagement recommendations.	No
Provide planning support between internal and external partners.	No
Provide real-time actionable geolocation information.	No
Provide target recommendations which meet leadership objectives.	No
Provide targeting products and targeting support as designated.	No
Provide time sensitive targeting support.	No
Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.	No
Recommend refinement, adaption, termination, and execution of operational plans as appropriate.	No

Review appropriate information sources to determine validity and relevance of information gathered.	No
Reconstruct networks in diagram or report format.	Yes
Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects.	No
Report intelligence-derived significant network events and intrusions.	No
Request discipline-specific processing, exploitation, and disseminate information collected using discipline's collection assets and resources in accordance with approved guidance and/or procedures.	No
Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.	Yes
Review and comprehend organizational leadership objectives and guidance for planning.	No
Review capabilities of allocated collection assets.	No
Review intelligence collection guidance for accuracy/applicability.	No
Review list of prioritized collection requirements and essential information.	No
Review and update overarching collection plan, as required.	No
Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities.	No
Revise collection matrix based on availability of optimal assets and resources.	No
Sanitize and minimize information to protect sources and methods.	No
Scope the cyber intelligence planning effort.	No
Serve as a conduit of information from partner teams by identifying subject matter experts who can assist in the investigation of complex or unusual situations.	No
Serve as a liaison with external partners.	No
Solicit and manage to completion feedback from requestors on quality, timeliness, and effectiveness of collection against collection requirements.	No
Specify changes to collection plan and/or operational environment that necessitate re-tasking or re-directing of collection assets and resources.	No
Specify discipline-specific collections and/or taskings that must be executed in the near term.	No
Submit information requests to collection requirement management section for processing as collection requests.	No
Submit or respond to requests for deconfliction of cyber operations.	No
Support identification and documentation of collateral effects.	Yes
Synchronize cyber international engagement activities and associated resource requirements as appropriate.	No
Synchronize cyber portions of security cooperation plans.	No
Synchronize the integrated employment of all available organic and partner intelligence collection assets using available collaboration capabilities and techniques.	No
Test and evaluate locally developed tools for operational use.	No
Test internal developed tools and techniques against target tools.	No

Track status of information requests, including those processed as collection requests and production requirements, using established procedures.	No
Translate collection requests into applicable discipline-specific collection requirements.	No
Use feedback results (e.g., lesson learned) to identify opportunities to improve collection management efficiency and effectiveness.	No
Validate requests for information according to established criteria.	No
Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	No
Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence requirements are accurate and up-to-date.	No
Document lessons learned that convey the results of events and/or exercises.	No
Advise managers and operators on language and cultural issues that impact organization objectives.	No
Analyze and process information using language and/or cultural expertise.	No
Assess, document, and apply a target's motivation and/or frame of reference to facilitate analysis, targeting and collection opportunities.	No
Collaborate across internal and/or external organizational lines to enhance collection, analysis and dissemination.	No
Conduct all-source target research to include the use of open source materials in the target language.	No
Conduct analysis of target communications to identify essential information in support of organization objectives.	No
Perform quality review and provide feedback on transcribed or translated materials.	No
Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing.	No
Identify cyber threat tactics and methodologies.	No
Identify target communications within the global network.	No
Maintain awareness of target communication tools, techniques, and the characteristics of target communication networks (e.g., capacity, functionality, paths, critical nodes) and their potential implications for targeting, collection, and analysis.	No
Provide feedback to collection managers to enhance future collection and analysis.	No
Perform foreign language and dialect identification in initial source data.	Yes
Perform or support technical network analysis and mapping.	No
Provide requirements and feedback to optimize the development of language processing tools.	No
Perform social network analysis and document as appropriate.	No
Scan, identify and prioritize target graphic (including machine-to-machine communications) and/or voice language material.	No
Tip critical or time-sensitive information to appropriate customers.	No
Transcribe target voice materials in the target language.	No
Translate (e.g., verbatim, gist, and/or summaries) target graphic material.	No

Translate (e.g., verbatim, gist, and/or summaries) target voice material.	No
Identify foreign language terminology within computer programs (e.g., comments, variable names).	No
Provide near-real time language analysis support (e.g., live operations).	No
Identify cyber/technology-related terminology in the target language.	No
Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations.	No
Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.	No
Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.	No
Liaise with regulatory and accrediting bodies.	No
Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.	No
Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.	No
Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.	No
Work with business teams and senior management to ensure awareness of “best practices” on privacy and data security issues.	No
Work with organization senior management to establish an organization-wide Privacy Oversight Committee	No
Serve in a leadership role for Privacy Oversight Committee activities	No
Collaborate on cyber privacy and security policies and procedures	No
Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation	No
Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations	No
Provide strategic guidance to corporate officers regarding information resources and technology	No
Assist the Security Officer with the development and implementation of an information infrastructure	No
Coordinate with the Corporate Compliance Officer regarding procedures for documenting and reporting self-disclosures of any evidence of privacy violations.	No
Work cooperatively with applicable organization units in overseeing consumer information access rights	No

Serve as the information privacy liaison for users of technology systems	No
Act as a liaison to the information systems department	No
Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations	No
Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties	No
Conduct on-going privacy training and awareness activities	No
Work with external affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues—and to manage company participation in public events related to privacy and data security	No
Work with organization administration, legal counsel and other related parties to represent the organization's information privacy interests with external parties, including government bodies, which undertake to adopt or amend privacy legislation, regulation or standard.	No
Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee	No
Work with External Affairs to respond to press and other inquiries regarding concern over consumer and employee data	No
Provide leadership for the organization's privacy program	No
Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization	No
Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce and for all business associates in cooperation with Human Resources, the information security officer, administration and legal counsel as applicable	No
Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures	No
Resolve allegations of noncompliance with the corporate privacy policies or notice of information practices	No
Develop and coordinate a risk management and compliance framework for privacy	No
Undertake a comprehensive review of the company's data and privacy projects and ensure that they are consistent with corporate privacy and data security goals and policies.	No
Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations	No
Establish a process for receiving, documenting, tracking, investigating and acting on all complaints concerning the organization's privacy policies and procedures	No
Establish with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity	No

Provide leadership in the planning, design and evaluation of privacy and security related projects	No
Establish an internal privacy audit program	No
Periodically revise the privacy program considering changes in laws, regulatory or company policy	No
Provide development guidance and assist in the identification, implementation and maintenance of organization information privacy policies and procedures in coordination with organization management and administration and legal counsel	No
Assure that the use of technologies maintains, and does not erode, privacy protections on use, collection and disclosure of personal information	No
Monitor systems development and operations for security and privacy compliance	No
Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected	No
Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions	No
Review all system-related information security plans to ensure alignment between security and privacy practices	No
Work with all organization personnel involved with any aspect of release of protected information to ensure coordination with the organization's policies, procedures and legal requirements	No
Account for and administer individual requests for release or disclosure of personal and/or protected information	Yes
Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements	Yes
Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed	No
Act as, or work with, counsel relating to business partner contracts	No
Mitigate effects of a use or disclosure of personal information by employees or business partners	No
Develop and apply corrective action procedures	No
Administer action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel	No
Support the organization's privacy compliance program, working closely with the Privacy Officer, Chief Information Security Officer, and other business leaders to ensure compliance with federal and state privacy laws and regulations	No
Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations	Yes

Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units	Yes
Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices	No
Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations	Yes
Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials	Yes
Develop and maintain appropriate communications and training to promote and educate all workforce members and members of the Board regarding privacy compliance issues and requirements, and the consequences of noncompliance	No
Determine business partner requirements related to the organization's privacy program.	No
Establish and administer a process for receiving, documenting, tracking, investigating and taking corrective action as appropriate on complaints concerning the company's privacy policies and procedures.	No
Cooperate with the relevant regulatory agencies and other legal entities, and organization officers, in any compliance reviews or investigations.	No
Perform ongoing privacy compliance monitoring activities.	No
Monitor advancements in information privacy technologies to ensure organization adoption and compliance.	No
Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations.	No
Appoint and guide a team of IT security experts.	No
Collaborate with key stakeholders to establish a cybersecurity risk management program.	No
Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework.	No
Establish a risk management strategy for the organization that includes a determination of risk tolerance.	No
Identify the missions, business functions, and mission/business processes the system will support.	No
Identify stakeholders who have a security interest in the development, implementation, operation, or sustainment of a system.	No
Identify stakeholders who have a security interest in the development, implementation, operation, or sustainment of a system.	No
Identify stakeholder assets that require protection.	No
Conduct an initial risk assessment of stakeholder assets and update the risk assessment on an ongoing basis.	No
Define the stakeholder protection needs and stakeholder security requirements.	No
Determine the placement of a system within the enterprise architecture.	No

Identify organization-wide common controls that are available for inheritance by organizational systems.	No
Conduct a second-level security categorization for organizational systems with the same impact level.	No
Determine the boundary of a system.	No
Identify the security requirements allocated to a system and to the organization.	No
Identify the types of information to be processed, stored, or transmitted by a system.	No
Categorize the system and document the security categorization results as part of system requirements.	No
Describe the characteristics of a system.	No
Register the system with appropriate organizational program/management offices.	No
Select the security controls for a system and document the functional description of the planned control implementations in a security plan.	No
Develop a strategy for monitoring security control effectiveness; coordinate the system-level strategy with the organization and mission/business process-level monitoring strategy.	No
Review and approve security plans.	No
Implement the security controls specified in a security plan or other system documentation.	No
Document changes to planned security control implementation and establish the configuration baseline for a system.	No
Develop, review, and approve a plan to assess the security controls in a system and the organization.	No
Assess the security controls in accordance with the assessment procedures defined in a security assessment plan.	No
Prepare a security assessment report documenting the issues, findings, and recommendations from the security control assessment.	No
Conduct initial remediation actions on security controls based on the findings and recommendations of a security assessment report; reassess remediated controls.	No
Prepare a plan of action and milestones based on the findings and recommendations of a security assessment report excluding any remediation actions taken.	No
Assemble an authorization package and submit the package to an authorizing official for adjudication.	No
Determine the risk from the operation or use of a system or the provision or use of common controls.	No
Identify and implement a preferred course of action in response to the risk determined.	No
Determine if the risk from the operation or use of the system or the provision or use of common controls, is acceptable.	No
Monitor changes to a system and its environment of operation.	No
Assess the security controls employed within and inherited by the system in accordance with an organization-defined monitoring strategy.	No
Respond to risk based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in a plan of action and milestones.	No

Update a security plan, security assessment report, and plan of action and milestones based on the results of a continuous monitoring process.	No
Report the security status of a system (including the effectiveness of security controls) to an authorizing official on an ongoing basis in accordance with the monitoring strategy.	No
Review the security status of a system (including the effectiveness of security controls) on an ongoing basis to determine whether the risk remains acceptable.	No
Implement a system disposal strategy which executes required actions when a system is removed from service.	No
Sponsor and promote continuous monitoring within the organization.	No
Assign staff as needed to appropriate continuous monitoring working groups.	No
Identify reporting requirements to support continuous monitoring activities.	No
Establish scoring and grading metrics to measure effectiveness of continuous monitoring program.	No
Determine how to integrate a continuous monitoring program into the organization's broader information security governance structures and policies.	No
Use continuous monitoring scoring and grading metrics to make information security investment decisions to address persistent issues.	No
Ensure that the continuous monitoring staff have the training and resources (e.g., staff and budget) needed to perform assigned duties.	No
Work with organizational risk analysts to ensure that continuous monitoring reporting covers appropriate levels of the organization.	No
Work with the organizational risk analysts to ensure risk metrics are defining realistically to support continuous monitoring.	No
Work with organizational officials to ensure continuous monitoring tool data provides situation awareness of risk levels.	No
Establish triggers for unacceptable risk thresholds for continuous monitoring data.	No
Work with organizational officials to establish system level reporting categories that can be used by the organization's continuous monitoring program.	No
Designate a qualified person to be responsible for the management and implementation of the continuous monitoring program.	No
Identify the continuous monitoring stakeholders and establish a process to keep them informed about the program.	No
Identify security oriented organization reporting requirements that are fulfilled by the continuous monitoring program.	No
Use the continuous monitoring data to make information security investment decisions to address persistent issues.	No
Define triggers within the continuous monitoring program that can be used to define unacceptable risk and result in action being taken to resolve.	No
Establish scoring and grading metrics to measure effectiveness of continuous monitoring program.	No

Work with security managers to establish appropriate continuous monitoring reporting requirements at the system level.	No
Use the continuous monitoring tools and technologies to assess risk on an ongoing basis.	No
Establish appropriate reporting requirements in adherence to the criteria identified in the continuous monitoring program for use in automated control assessment.	No
Use non-automated assessment methods where the data from the continuous monitoring tools and technologies is not yet of adequate sufficiency or quality.	No
Develop processes with the external audit group on how to share information regarding the continuous monitoring program and its impact on security control assessment.	No
Identify reporting requirements for use in automated control assessment to support continuous monitoring.	No
Determine how the continuous monitoring results will be used in ongoing authorization.	No
Establish continuous monitoring tools and technologies access control process and procedures.	No
Ensure that continuous monitoring tools and technologies access control is managed adequately.	No
Establish a process to provide technical help to continuous monitoring mitigators.	No
Coordinate continuous monitoring reporting requirements across various users.	No
Establish responsibilities for supporting implementation of each continuous monitoring tool or technology.	No
Establish liaison with scoring and metrics working group to support continuous monitoring.	No
Establish and operate a process to manage introduction of new risk to support continuous monitoring.	No
Establish continuous monitoring configuration settings issues and coordination sub-group.	No
Establish continuous monitoring tools and technologies performance measurement/management requirements.	No
Using scores and grades to motivate and assess performance while addressing concerns to support continuous monitoring	No
Work with security managers (i.e., system owners, information system security managers, information system security officers, etc.) to establish appropriate reporting requirements for continuous monitoring at the system level.	No
Use continuous monitoring tools to assess risk on an ongoing basis.	No
Use the continuous monitoring data to make information security investment decisions to address persistent issues.	No
Respond to issues flagged during continuous monitoring, escalate and coordinate a response.	No
Review findings from the continuous monitoring program and mitigate risks on a timely basis.	No

g. List of potential threats to your company that could exploit vulnerabilities of critical assets due to missing Cybersecurity Specialty Areas, Cybersecurity Work Roles, and Cybersecurity Tasks

1. Application attacks
2. Compromise Spread
3. Compromised Network Node
4. Compromised Workstation
5. Denial of Service
6. Disclosure of Confidential Information
7. Disgruntled Employee
8. Financial Theft
9. Human Error
10. Intelligence and Information Gathering
11. Loss of Accountability and Trust
12. Lost RFID tag
13. Malicious Actor
14. Malicious Changes
15. Malicious or Suspicious Traffic
16. Natural Disaster
17. Network-Related Attacks
18. System Error

h. List of potential risks for critical assets where Cybersecurity Specialty Areas, Cybersecurity Work Roles, and Cybersecurity Tasks are missing

· Use of outdated network protocols can lead to successful network-related attacks, compromising integrity of the information systems as well as the confidentiality of data flowing across the network
· Weak LAN encryption for network services can reveal user credentials to potential packet sniffing on the LAN, giving attackers access to IT systems and apps
· Attackers can leverage repudiation and integrity verification weaknesses and in the case of email communications, interception of messages is possible leading to a breach in confidentiality and to a loss of trust
· Weak authentication that can lead to potential impersonation and to unauthorized access of physical assets and resources.
· Identity theft not put in check, leading to potential impersonation and to unauthorized access of logical and physical assets and resources.
· Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view LDAP credentials in cleartext
· Lack of NTAP can lead to traffic congestion and delays due to IDS working in real-time and not on duplicate/mirrored packets, which can potentially lead to loss of services availability.
· Deep Inspection Firewalls are already configured and cover all of this firewall's capabilities

· Attackers can easily understand network topology and scan for vulnerable versions or Operating Systems using recon and scanning tools. Additionally they can perform DDoS attacks because ICMP echo requests are not disabled.
· Attackers can abuse the lack of source IP check to spoof their source IP address to match the IP address of an internal device, leading to security compromises.
· Since Cloudfare is deployed for DDoS mitigation, only internal attacks need to be mentioned - an attacker with internal network access or a compromised network node can perform SYN flood attacks leading to Denial of Service.
· Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view LDAP credentials in cleartext.
· The DES key used for encryption in SNMPv2 can be cracked with enough time, leading to malicious network activity and network disruption.
· Attackers can gain unauthorized access to DB which leads to a breach in confidentiality, and more potentially depending on the level of access the account they are using has.
· Keeping default account names makes it easier for attackers to guess the account name correctly and in turn makes it easier to brute-force the login.
· Uncapped session TTL and count can lead to session hijacking attacks as well as denial of service attacks on the DB by flooding it with requests.
· Any attacker with access to the network through a compromised network device can eavesdrop and intercept the traffic and view login credentials or other data in cleartext.
· Lack of integrity check for the configuration files, data files and other files before DB startup can lead to malicious code execution and more.
· Not clearing RAM or virtual memory can lead to code re-use attacks, or just data and code leakage in the case of a compromised system, which is a breach of confidentiality and help attackers in intel gathering.
· Attackers can gain unauthorized access to the app which leads to a breach in confidentiality, and more potentially depending on the level of access the account they compromise has.
· Attackers can potentially make unwanted and malicious changes to code leadings malicious code execution and more.
· Not following best security practices when coding can lead to successful attacks against apps.
· Not using identity hiding which is one of the benefits of EAP-TTLS, so the authenticator is aware of both the username that establishes the TLS channel in the first phase and the user authenticated in the second phase
· Attacker knows SSID of the router as it is discoverable, so he can perform different attacks and gain intel on the network's security posture. The attacker can also spoof access points SSID to trick guests.
· Someone with physical access to a workstation that uses bluetooth can take advantage of some weak authentication methods.
· Someone with access to an RFID tag can attempt to read data stored if it not well encrypted - passive RFID has weaker encryption than active RFID because the latter uses a battery.

i. List of recommended policies for each recommended Cybersecurity Specialty Area, Cybersecurity Work Role, or Cybersecurity Task that should be created to mitigate the identified risks

- Implement a PKI infrastructure to help with authentication, integrity validation, confidentiality.

- Implement MFA for all accounts that have access to sensitive information or escalated privileges.
- Use S/MIME for email confidentiality and integrity.
- Use Smart ID Cards for personnel authentication, authorization and physical security.
- Use Biometric Scanners to increase personnel authentication, authorization and physical security.
- Update the configuration of network systems that still use protocols with weak encryption.
- Providing users with physical tokens.
- Configure, implement and test DBIDS.
- Install Network Access Ports for congestion issues with IDS solutions
- Configure Unicast Reverse Path Forwarding (uRPF) on routers.
- Restrict the time window and/or the packet rate for an open TCP connection.
- Move from SNMPv2 to SNMPv3 as it offers more secure cryptographic suites for encryption, amongst other benefits.
- Configure TLS on DB servers to protect data in transit.
- Restrict Session TTL and session count for DB connections.
- Put logon restrictions in place, such as limited tries before account is locked.
- Use Federated Databases to handle large volumes of traffic by utilizing the load balancing capabilities it has to offer.
- Configure TLS or IPSec on app servers to protect app data in-transit.
- Restrict Session TTL and session count for app sessions.
- Minimize use of global variables, use thread-safe functions and ensure enforcement of ACLs.
- Disable SSID Broadcast on wireless network devices and provide clients and guest network users with SSID after getting approval.
- Configure EAP-TTLS to authenticate client connecting to the network.
- Consider switching to active RFID tags as they offer more secure encryption.
- Improve Incident Handling processes by preparing Incident Response Playbooks and categorizing them properly as well as making them easily accessible.
- Update Incident Response Playbooks regularly.
- Regularly revise your Business Continuity Plan.
- Regularly monitor logs using IDS software that generates alerts.
- Regularly tune the IDS software to get rid of false positives.
- Disable ICMP echo response on routers.
- Configure collection of Clustering Logs, System State Changes and Audit Security Label Changes.
- Backup copies of critical software.
- Configure Trusted Recovery for DBs.
- Clear virtual memory or RAM that previously stored that data.
- Implement Fuzzy Testing.
- Have Bluetooth communications setup on security Mode 4 and to fall back onto security Mode 3 if the former fails.

PART C - Security Risk Management Recommendations

Part - C1

Provide a list of recommended Prevention and Response controls, methods and policies and their implementation costs and benefits based on a risk management analysis from Parts A and B.

For HGA:

- Replacing the modem pool with a VPN server reduces probability of exploitation on vulnerabilities for all threats. In fact, VPN allows for a more secure remote access connection that employees can use more confidently. VPN provides confidentiality and integrity, as the traffic is tunneled, meaning that it is encrypted and travels the internet securely. This minimizes risk related to information disclosure or brokerage, and it also helps with controlling unauthorized access, all while reducing likelihood of network-related attacks that were possible on the previous modem pools.
- Adding a screened subnet with DMZ enforces security controls, and certainly helps with access control and organizing the network architecture, while limiting damage in case of an intrusion.
- Use third party Denial of Service Mitigation services, such as Cloudflare can prove very useful against DoS attacks, helping reduce mostly interruption of operations.
- Regular patch network vulnerabilities.
- Regular and timely vulnerability scanning as well as patching should be implemented.
- Deploy PKI infrastructure.
- Implement MFA for users, app accounts and any access to sensitive information or escalated privileges.
- Use OTP or RSA tokens as part of the MFA process.
- Implement Biometric security.
- Employees should learn to be more cautious regarding security, and should understand the importance and the weight behind security. Give them some incentive to do so with a reward program perhaps.
- All transactions related to HGAs financial resources (such as equity or bond sales, to employee salary distribution, and others) should go through an approval process by two people so that there is no single point of failure.
- Business Documents, Memos and Reports should be encrypted with up-to-date cryptographic schemes and stored securely with high-privilege access controls and servers should be located in the DMZ to further increase detection mechanisms.
- Develop a proper disaster recovery plan if you cannot fix the facilities or move to newer ones, as they have a higher risk of destruction due to natural disasters.

For HIC:

- Implement a PKI infrastructure to help with authentication, integrity validation, confidentiality.
- Implement MFA for all accounts that have access to sensitive information or escalated privileges.
- Use S/MIME for email confidentiality and integrity.
- Use Smart ID Cards for personnel authentication, authorization and physical security.

- Use Biometric Scanners to increase personnel authentication, authorization and physical security.
- Update the configuration of network systems that still use protocols with weak encryption.
- Providing users with physical tokens.
- Configure, implement and test DBIDS.
- Install Network Access Ports for congestion issues with IDS solutions
- Configure Unicast Reverse Path Forwarding (uRPF) on routers.
- Restrict the time window and/or the packet rate for an open TCP connection.
- Move from SNMPv2 to SNMPv3 as it offers more secure cryptographic suites for encryption, amongst other benefits.
- Configure TLS on DB servers to protect data in transit.
- Restrict Session TTL and session count for DB connections.
- Put logon restrictions in place, such as limited tries before account is locked.
- Use Federated Databases to handle large volumes of traffic by utilizing the load balancing capabilities it has to offer.
- Configure TLS or IPSec on app servers to protect app data in-transit.
- Restrict Session TTL and session count for app sessions.
- Minimize use of global variables, use thread-safe functions and ensure enforcement of ACLs.
- Disable SSID Broadcast on wireless network devices and provide clients and guest network users with SSID after getting approval.
- Configure EAP-TTLS to authenticate client connecting to the network.
- Consider switching to active RFID tags as they offer more secure encryption.
- Improve Incident Handling processes by preparing Incident Response Playbooks and categorizing them properly as well as making them easily accessible.
- Update Incident Response Playbooks regularly.
- Regularly revise your Business Continuity Plan.
- Regularly monitor logs using IDS software that generates alerts.
- Regularly tune the IDS software to get rid of false positives.
- Disable ICMP echo response on routers.
- Configure collection of Clustering Logs, System State Changes and Audit Security Label Changes.
- Backup copies of critical software.
- Configure Trusted Recovery for DBs.
- Clear virtual memory or RAM that previously stored that data.
- Implement Fuzzy Testing.
- Do not allow the use of Bluetooth devices unless truly necessary – if there is a business need for it.
- Have Bluetooth communications setup on security Mode 4 and to fall back onto security Mode 3 if the former fails.

Part - C2

Provide the total cost and benefit in $ for the recommended controls, methods and policies based on your security risk management analysis in Parts A and B above

For HGA:

Current Residual Risk	Residual Risk with New Controls	Residual Risk Reduction - Security Risk Benefit
$6,446,000	$1,190,235	$5,255,765

Cost/Benefit Ratio computation:

Residual Risk Reduction - Security Risk Benefit	New Controls Costs - Security Risk Budget Cost	Cost/Benefit Ratio
$5,255,765	$761,000	0.144793384

According to the Cost/Benefit Ratio, HGA's best bet is on a Mixed strategy, as the benefits from reducing residual risk, all while taking into consideration the new controls implementation costs and budget, have proven to be superior to other strategies. One thing to keep in mind is that the budget and costs only include monetary value, and that it is important to consider Time as a resource as well, to see if HGA has time to implement all these new security controls. However, HGA doesn't have to implement everything all at once and can manage their time by looking closer at which security controls have the greatest risk reduction factors and start with those.

For HIC:

Current Residual Risk	Residual Risk with New Controls	Residual Risk Reduction - Security Risk Benefit
$23,592,000	$7,820,336	$15,771,664

Cost/Benefit Ratio computation:

Residual Risk Reduction - Security Risk Benefit	New Controls Costs - Security Risk Budget Cost	Cost/Benefit Ratio
$15,771,664	$6,561,499	0.416030864

HIC would greatly benefit from implementing the suggested security controls and risk mitigation technologies. The residual risk would be significantly reduced by approximately 67% for a total of $15.7M. Again, similarly to HGA, the budget and costs for HIC only include the dollar value of the implementations, and it is important to consider Time as a resource as well. As a previous employee of HIC, I know that time is a very limited resource for the security team, as it is a relatively small team considering the company assets that are in play. Nevertheless, HIC doesn't have to implement everything all at once and can manage their time by looking closer at which security controls have the greatest risk reduction factors and start with those.

Part - C3

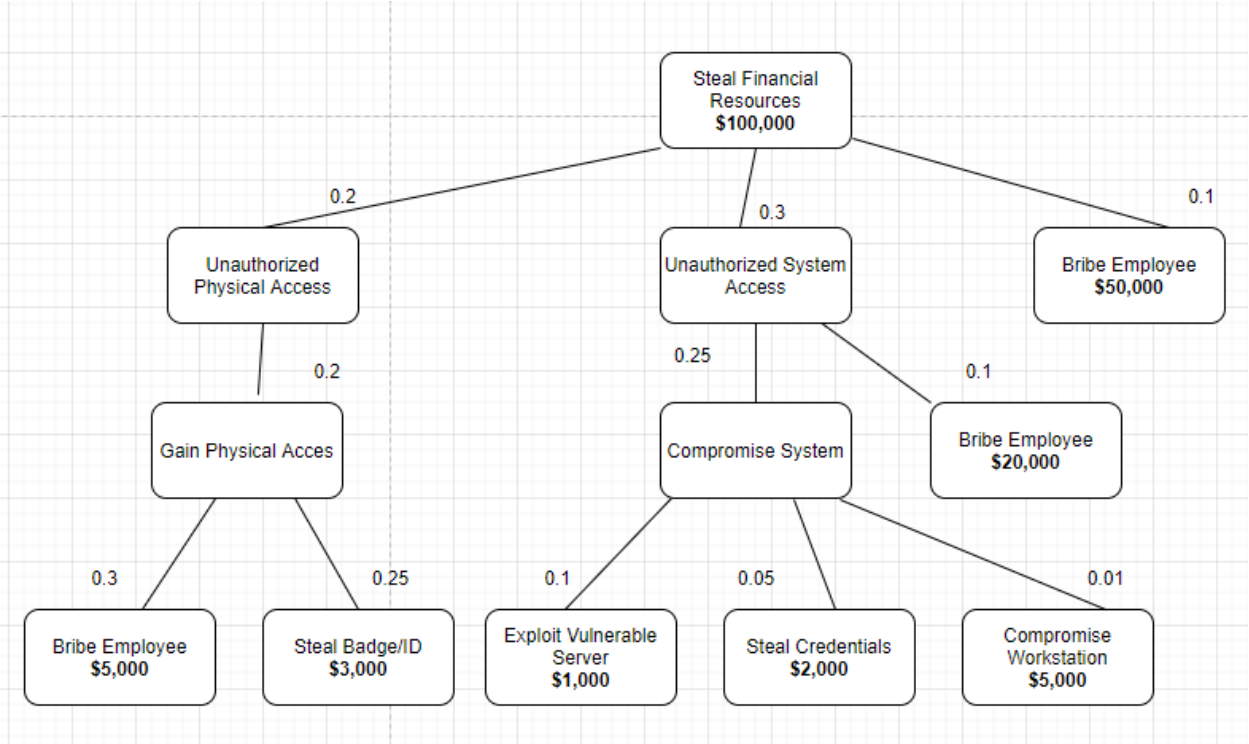
Compare your proposed security controls, methods and policies budget for HGA (which is based on security risk assessment in Part A) with the proposed security controls, methods and policies budget for your company (which is based on security risk implementation plan in Part B), adjusting for industry, mission, scale, threat environment and workforce differences between HGA and your company.

NOTE: Network Topology for HGA and HIC is in the Appendix

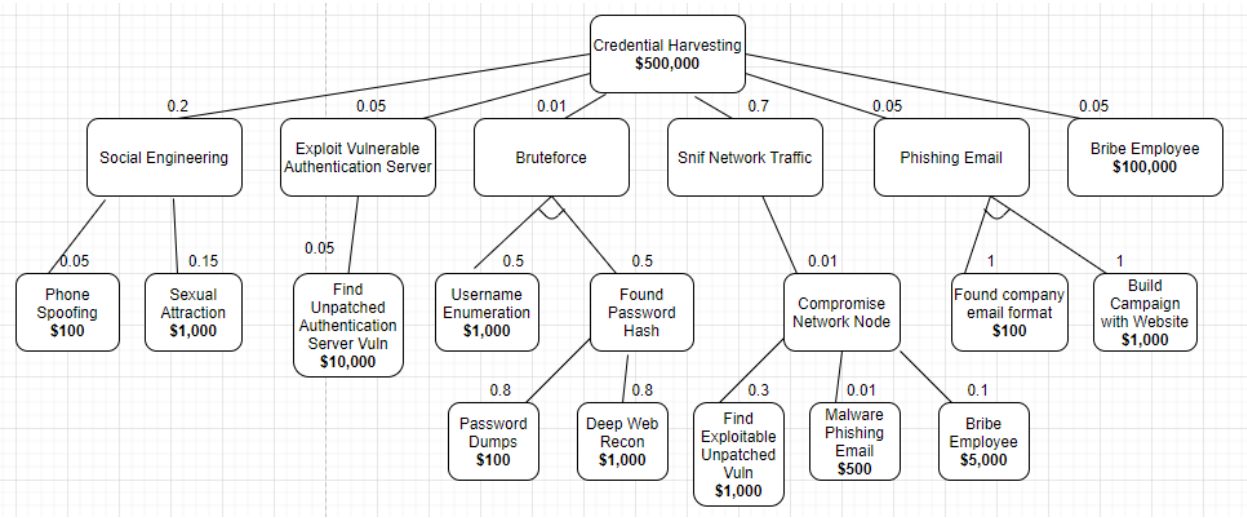
Point of Comparison	HGA	HIC
Industry	Governmental	Investments/Banking/Financial
Mission	Distribute funds and salaries in form of paychecks to US Government employees and beneficiaries	Investing on behalf of clients is HIC's primary goal - across asset classes and around the world, the investment teams identify and exploit long-term opportunities and develop solutions that both anticipate and respond to client needs.
Geographic Presence	USA	Boston, Los Angeles, London, Amsterdam, Singapore, Sydney
Number of Employees	1000	600
Threat Agents	Competing Nation States, Terrorist Groups, Black Hat Hackers, Hacker Groups, Hacktivists, Natural Disasters	Competing Companies, Black Hat Hackers, Hacker Groups, Hacktivists, Disgruntled Employees, Natural Distaters
Critical Assets Total Value ($)	$6,446,000	$70,163,000,000
Residual Security Risk ($)	$6,446,000	$23,592,000
Budget for Risk Controls ($)	$761,000	$6,561,499
$ Security Budget/ $ Security Risk Improvement	0.144793384	0.416030864
$ Security Budget/ $ Critical Assets	0.11805771	0.00009352
$ Security Budget/ employee	$761	$10,935.83

Attack Tree Samples:

For HGA:



For HIC:



Vulnerabilities and Exploitation Probabilities:

For HGA:

Vulnerability	**Exploitation Probability (%)**
Vulnerabilities Related to Payroll Fraud	40

Falsified Time Sheets	45
Unauthorized Access	55
Bogus Time and Attendance Applications	40
Unauthorized Modifications of Time and Attendance Sheets	30
Vulnerabilities Related to Payroll Errors	40
Vulnerabilities Related to Continuity of Operations	45
COG Contingency Planning	50
Division Contingency Planning	50
Virus Prevention	40
Accidental Corruption and Loss of Data	60
Vulnerabilities Related to Information Disclosure or Brokerage	40
Network-Related Vulnerabilities	50

For HIC:

Vulnerability	Exploitation Probability (%)
Unauthorized Access	10
Impersonation	15
Weak Authentication	15
Repudiation	10
Network-Related Vulnerabilities	10
Breach of Confidentiality and Integrity	5
Credential Harvesting	10
Network Congestion	5
Poor IDS/IPS Performance	2
Weak Protection against Recon and Scanning Tools	25
Breach of Confidentiality	5
ICMP Vulnerabilities	15
SYN Flooding	10
IP Address Spoofing	10
Uncapped TTL and Session Count	5

Unlimited Logon Attempts	15
Loss or Corruption of Software	1
No Integrity Validation	5
Outdated Policies	10
Unpartitioned Apps	2
Software Library Vulnerabilities	2
Weak Access Control	5
Username Enumeration	25
No Load Balancing	5
Virtual Memory Vulnerabilities	2
Software and Coding Vulnerabilities.	5
Weak Encryption	15
Network Device Publicly Discoverable	30

Cybersecurity Workforce Recommendations:

For HGA:

- Network Engineer & SysAdmin: Implement VPN for remote employee login – recommended to be in IPSec transport mode for end-to-end security.
- Network Architect: Adding a screened subnet with DMZ enforces security controls, and certainly helps with access control and organizing the network architecture, while limiting damage in case of an intrusion.
- CISO: Use third party Denial of Service Mitigation services, such as Cloudflare can prove very useful against DoS attacks, helping reduce mostly interruption of operations.
- Network Security Engineer: Regularly patch network vulnerabilities.
- Network Security Engineer: Regular and timely vulnerability scanning as well as patching should be implemented.
- DevOps and IAM Team: Deploy PKI infrastructure.
- IAM team: Implement MFA for users, app accounts and any access to sensitive information or escalated privileges.
- IAM team: Use OTP or RSA tokens as part of the MFA process.
- IAM team: Implement Biometric security.
- Ethics Team and Security Trainers: Employees should learn to be more cautious regarding security, and should understand the importance and the weight behind security. Give them some incentive to do so with a reward program perhaps.
- Security Risk Manager and Business Owner: All transactions related to HGAs financial resources (such as equity or bond sales, to employee salary distribution, and others) should go through an approval process by two people so that there is no single point of failure.
- DBA and DB Devs: Business Documents, Memos and Reports should be encrypted with up-to-date cryptographic schemes and stored securely with high-privilege access controls and servers should be located in the DMZ to further increase detection mechanisms.

- DRP and IR team: Develop a proper disaster recovery plan if you cannot fix the facilities or move to newer ones, as they have a higher risk of destruction due to natural disasters.

For HIC:

- Software Devs and IAM team: Implement a PKI infrastructure to help with authentication, integrity validation, confidentiality.
- IAM Team and SysAdmin: Implement MFA for all accounts that have access to sensitive information or escalated privileges.
- Network Security Engineer: Use S/MIME for email confidentiality and integrity.
- Physical Security Team: Use Smart ID Cards for personnel authentication, authorization and physical security.
- Physical Security Team: Use Biometric Scanners to increase personnel authentication, authorization and physical security.
- Network Engineering Team: Update the configuration of network systems that still use protocols with weak encryption.
- IAM and Risk Management Team: Providing users with physical tokens.
- DBA and DB Devs: Configure, implement and test DBIDS.
- Network Security Engineer: Install Network Access Ports for congestion issues with IDS solutions
- Network Engineering Team: Configure Unicast Reverse Path Forwarding (uRPF) on routers.
- Network Security Engineer: Restrict the time window and/or the packet rate for an open TCP connection.
- Network Security Manager: Move from SNMPv2 to SNMPv3 as it offers more secure cryptographic suites for encryption, amongst other benefits.
- DBA and DB Devs: Configure TLS on DB servers to protect data in transit.
- DBA and DB Devs: Restrict Session TTL and session count for DB connections.
- DBA and DB Devs: Put logon restrictions in place, such as limited tries before account is locked.
- DBA and DB Devs: Use Federated Databases to handle large volumes of traffic by utilizing the load balancing capabilities it has to offer.
- DevOps and System Owners: Configure TLS or IPSec on app servers to protect app data in-transit.
- SysAdmin and System Owners: Restrict Session TTL and session count for app sessions.
- Software Developers: Minimize use of global variables, use thread-safe functions and ensure enforcement of ACLs.
- Network Engineering Team: Disable SSID Broadcast on wireless network devices and provide clients and guest network users with SSID after getting approval.
- Network Security Engineer and Manager: Configure EAP-TTLS to authenticate client connecting to the network.
- IAM and Physical Security Team: Consider switching to active RFID tags as they offer more secure encryption.
- Head of IR and DRP: Improve Incident Handling processes by preparing Incident Response Playbooks and categorizing them properly as well as making them easily accessible.
- Head of IR and DRP: Update Incident Response Playbooks regularly.
- Head of IR and DRP: Regularly revise your Business Continuity Plan.

- SIEM Engineer: Regularly monitor logs using IDS software that generates alerts.
- SIEM Engineer: Regularly tune the IDS software to get rid of false positives.
- Network Security Engineer: Disable ICMP echo response on routers.
- DevOps and DB Devs: Configure collection of Clustering Logs, System State Changes and Audit Security Label Changes.
- DBA and Software Developers: Backup copies of critical software.
- DBA and DB Devs: Configure Trusted Recovery for DBs.
- Software Developers and Coding Team: Clear virtual memory or RAM that previously stored that data.
- Pen-testers: Implement Fuzzy Testing.
- Network Engineers and Cyber Policy and Strategy Planners: Have Bluetooth communications setup on security Mode 4 and to fall back onto security Mode 3 if the former fails.

PART D - Appendix

Appendix 1

Appendix A – Security Risk Prevention Strategy Calculations

A1 - Residual Asset Security Risk (Phase 1)

Risk of A1=
5000000*[(40+50+50+25+60+15+60+15+15+15+15+15+70+15+70+20+50+20+65+75+15+15+30+65+80)%] = 48250000 > 5000000 (A1's Value) Therefore, Risk of A1 = 5000000 (total loss of asset).

Risk of A21 =
450000*[(40+50+50+25+60+15+60+15+15+15+15+15+70+15+70+20+50+20+65+75+15+15+30+65+80)%] = 4342500 > 450000 (A21's Value) Therefore, Risk of A21 = 450000 (total loss of asset).

Risk of A24=
60000*[(40+50+50+25+60+15+60+15+15+15+15+15+70+15+70+20+50+20+65+75+15+15+30+65+80)%] = 579000 > 60000 (A24's Value) Therefore, Risk of A24 = 60000 (total loss of asset).

Risk of A25=
6000*[(40+50+50+25+60+15+60+15+15+15+15+15+70+15+70+20+50+20+65+75+15+15+30+65+80)%] = 57900 > 6000 (A25's Value) Therefore, Risk of A25 = 6000 (total loss of asset).

Risk of A27=
30000*[(40+50+50+25+60+15+60+15+15+15+15+15+70+15+70+20+50+20+65+75+15+15+30+65+80)%] = 289500 > 30000 (A27's Value) Therefore, Risk of A27 = 30000 (total loss of asset).

Risk of A3=
400000*[(40+50+50+25+60+15+60+15+15+15+15+15+70+15+70+20+50+20+65+75+15+15+30+65+80)%] = 3860000 > 400000 (A3's Value) Therefore, Risk of A3 = 400000 (total loss of asset).

Risk of A7=
500000*[(40+50+50+25+60+15+60+15+15+15+15+15+70+15+70+20+50+20+65+75+15+15+30+65+80)%] = 4825000 > 500000 (A7's Value) Therefore, Risk of A7 = 500000 (total loss of asset).

A2 - Vulnerability Security Risk (Phase 1)

Risk due to T1V12 = 5000000*[(40+50+50+25+60)%] + 450000*[(40+50+50+25+60)%] + 60000*[(40+50+50+25+60)%] + 400000*[(40+50+50+25+60)%] + 500000*[(40+50+50+25+60)%] + 6000*[(40+50+50+25+60)%] + 30000*[(40+50+50+25+60)%] = 14503500

Risk due to T3V34 = 5000000*[(15+60+15+15+15)%] + 450000*[(15+60+15+15+15)%] + 60000*[(15+60+15+15+15)%] + 400000*[(15+60+15+15+15)%] + 500000*[(15+60+15+15+15)%])%] + 6000*[(15+60+15+15+15)%] + 30000*[(15+60+15+15+15)%] = $7,735,200

Risk due to T4V4 = 5000000*[(15+15+70+15+70)%] + 450000*[(15+15+70+15+70)%] + 60000*[(15+15+70+15+70)%] + 400000*[(15+15+70+15+70)%] + 500000*[(15+15+70+15+70)%] + 6000*[(15+15+70+15+70)%] + 30000*[(15+15+70+15+70)%] = $11,925,100

Risk due to T5V5 = 5000000*[(20+50+20+65+75)%] + 450000*[(20+50+20+65+75)%] + 60000*[(20+50+20+65+75)%] + 400000*[(20+50+20+65+75)%] + 500000*[(20+50+20+65+75)%] + 6000*[(20+50+20+65+75)%] + 30000*[(20+50+20+65+75)%] = $14,825,800

Risk due to T7V7 = 5000000*[(15+15+30+65+80)%] + 450000*[(15+15+30+65+80)%] + 60000*[(15+15+30+65+80)%] + 400000*[(15+15+30+65+80)%] + 500000*[(15+15+30+65+80)%] + 6000*[(15+15+30+65+80)%] + 30000*[(15+15+30+65+80)%] = $15,214,300

A3 - Residual Asset Security Risk (Phase 2)

Risk of A1=
5000000*[(10+15+15+10+15+15+30+15+15+15+15+15+20+15+10+5+10+5+25+15+15+15+15+20+25)%] = 19,000,000 > 5000000 (A1's Value) Therefore, Risk of A1 = 5000000 (total loss of asset).

Risk of A21 =
450000*[(10+15+15+10+15+15+30+15+15+15+15+15+20+15+10+5+10+5+25+15+15+15+15+20+25)%] = 1,710,000 > 450000 (A21's Value) Therefore, Risk of A21 = 450000 (total loss of asset).

Risk of A24=
60000*[(10+15+15+10+15+15+30+15+15+15+15+15+20+15+10+5+10+5+25+15+15+15+15+20+25)%] = 228,000 > 60000 (A24's Value) Therefore, Risk of A24 = 60000 (total loss of asset).

Risk of A25=
6000*[(10+15+15+10+15+15+30+15+15+15+15+15+20+15+10+5+10+5+25+15+15+15+15+20+25)%] = 22,800 > 6000 (A25's Value) Therefore, Risk of A25 = 6000 (total loss of asset).

Risk of A27=
30000*[(10+15+15+10+15+15+30+15+15+15+15+15+20+15+10+5+10+5+25+15+15+15+15+20+25)%] = 114,000 > 30000 (A27's Value) Therefore, Risk of A27 = 30000 (total loss of asset).

Risk of A3=
400000*[(10+15+15+10+15+15+30+15+15+15+15+15+20+15+10+5+10+5+25+15+15+15+15+20+25)%] = 1,520,000 > 400000 (A3's Value) Therefore, Risk of A3 = 400000 (total loss of asset).

Risk of A7=
500000*[(10+15+15+10+15+15+30+15+15+15+15+15+20+15+10+5+10+5+25+15+15+15+15+20+25)%] = 1,900,000 > 500000 (A7's Value) Therefore, Risk of A7 = 500000 (total loss of asset).

Residual Risk of all Assets = 6446000

A4 - Vulnerability Security Risk (Phase 2)

Risk due to T1V12 = 5000000*(10+15+15+10+15)% + 450000*(10+15+15+10+15)% + 60000*(10+15+15+10+15)% + 400000*(10+15+15+10+15)% + 500000*(10+15+15+10+15)% + 6000*(10+15+15+10+15)% + 30000*(10+15+15+10+15)% = $4,189,900

Risk due to T3V34 = 5000000*(15+30+15+15+15)% + 450000*(15+30+15+15+15)% + 60000*(15+30+15+15+15)% + 400000*(15+30+15+15+15)% + 500000*(15+30+15+15+15)% + 6000*(15+30+15+15+15)% + 30000*(15+30+15+15+15)% = $5,801,400

Risk due to T4V4 = 5000000*(15+15+20+15+10)% + 450000*(15+15+20+15+10)% + 60000*(15+15+20+15+10)% + 400000*(15+15+20+15+10)% + 500000*(15+15+20+15+10)% + 6000*(15+15+20+15+10)% + 30000*(15+15+20+15+10)% = $4,834,500

Risk due to T5V5 = 5000000*(5+10+5+25+15)% + 450000*(5+10+5+25+15)% + 60000*(5+10+5+25+15)% + 400000*(5+10+5+25+15)% + 500000*(5+10+5+25+15)% + 6000*(5+10+5+25+15)% + 30000*(5+10+5+25+15)% = $3,867,600

Risk due to T7V7 = 5000000*(10+15+15+20+25)% + 450000*(10+15+15+20+25)% + 60000*(10+15+15+20+25)% + 400000*(10+15+15+20+25)% + 500000*(10+15+15+20+25)% + 6000*(10+15+15+20+25)% + 30000*(10+15+15+20+25)% = $5,479,100

Appendix B – Security Risk Response Strategy Calculations

Appendix B.xlsx

Double click on the Icon above to see calculations in Excel.

Appendix C – Mixed Security Risk Strategy Calculations


Appendix C.xlsx

Double click on the Icon above to see calculations in Excel.

Appendix D – Strategy Budget Estimates

D1 - Risk Prevention Strategy (IX)

Controls	Estimated Budget Required
Controls Mitigating Vulnerabilities Related to Payroll	250,000
Controls Mitigating Payroll Error	10,000
Controls Mitigating Vulnerabilities Related to Continuity of Operations	20,000
Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of Information	50,000
Controls Mitigating Vulnerabilities Related to Network-Related Attacks	100,000
Controls Mitigating VPN-Related Vulnerabilities	50,000
VPN and DMZ addition	36,000
Denial of Service Mitigation services	35,000
TOTAL BUDGET	**$551,000**

D2 - Risk Response Strategy (X)

Controls	Estimated Budget Required
Controls Mitigating Vulnerabilities Related to Payroll	260,000
Controls Mitigating Payroll Error	15,000
Controls Mitigating Vulnerabilities Related to Continuity of Operations	25,000
Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of Information	60,000
Controls Mitigating Vulnerabilities Related to Network-Related Attacks	130,000
Controls Mitigating VPN-Related Vulnerabilities	100,000
VPN and DMZ addition	36,000
Denial of Service Mitigation services	35,000

Dual Approval System for Financial Resources Processes	50,000

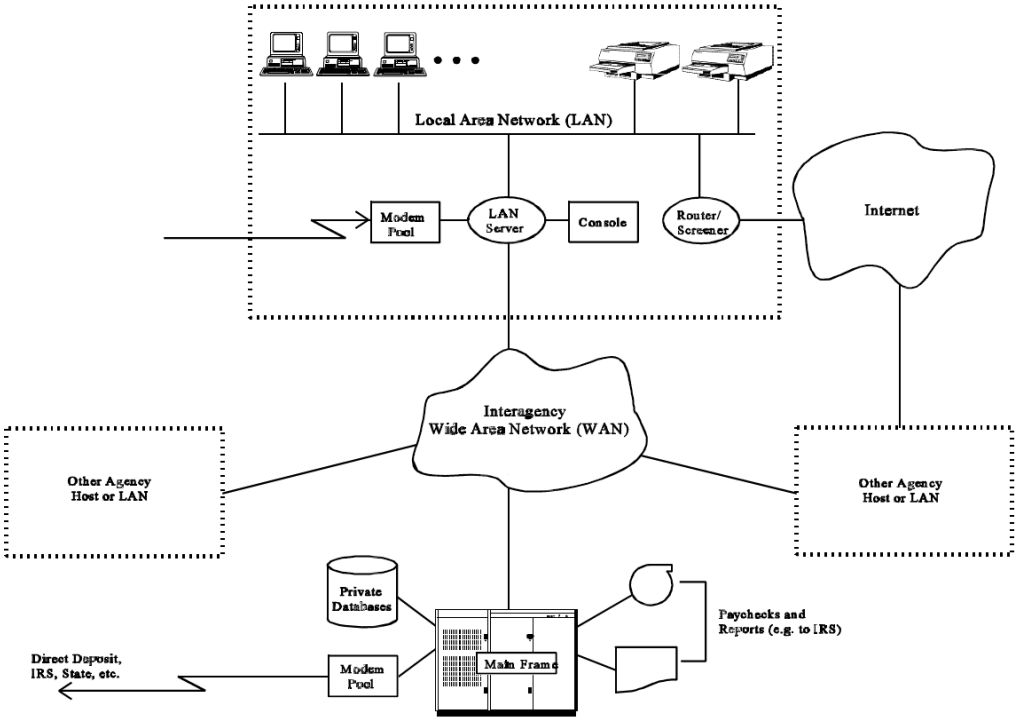
D3 - Mixed Risk Strategy (XI)

Controls	Estimated Budget Required
Controls Mitigating Vulnerabilities Related to Payroll	260,000
Controls Mitigating Payroll Error	15,000
Controls Mitigating Vulnerabilities Related to Continuity of Operations	25,000
Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of Information	60,000
Controls Mitigating Vulnerabilities Related to Network-Related Attacks	130,000
Controls Mitigating VPN-Related Vulnerabilities	100,000
VPN and DMZ addition	36,000
Denial of Service Mitigation services	35,000
Dual Approval System for Financial Resources Processes	50,000
Incident Response Plan for physical and environmental accidents as well as intrusions or breaches	30,000
Additional Servers Encryption and Least Privilege Access Controls	20,000
TOTAL BUDGET	**$761,000**

Appendix 2

Detailed Network Topology for HGA

HGA has a straightforward system topology and infrastructure that is portrayed in the image below. Most devices such as PCs and printers are connected to a LAN server. The LAN server is also responsible for connecting modem pools as well as special consoles that employees use to log-in to HGA's system. The main security control mechanism that the LAN server deploys is an Access Control infrastructure, and the access is given after written consent. For internet access, HGA has a main internet-facing router and for HGA to connect with other agencies, as well as a mainframe, their LAN server is connected to a WAN that offers all of the above.

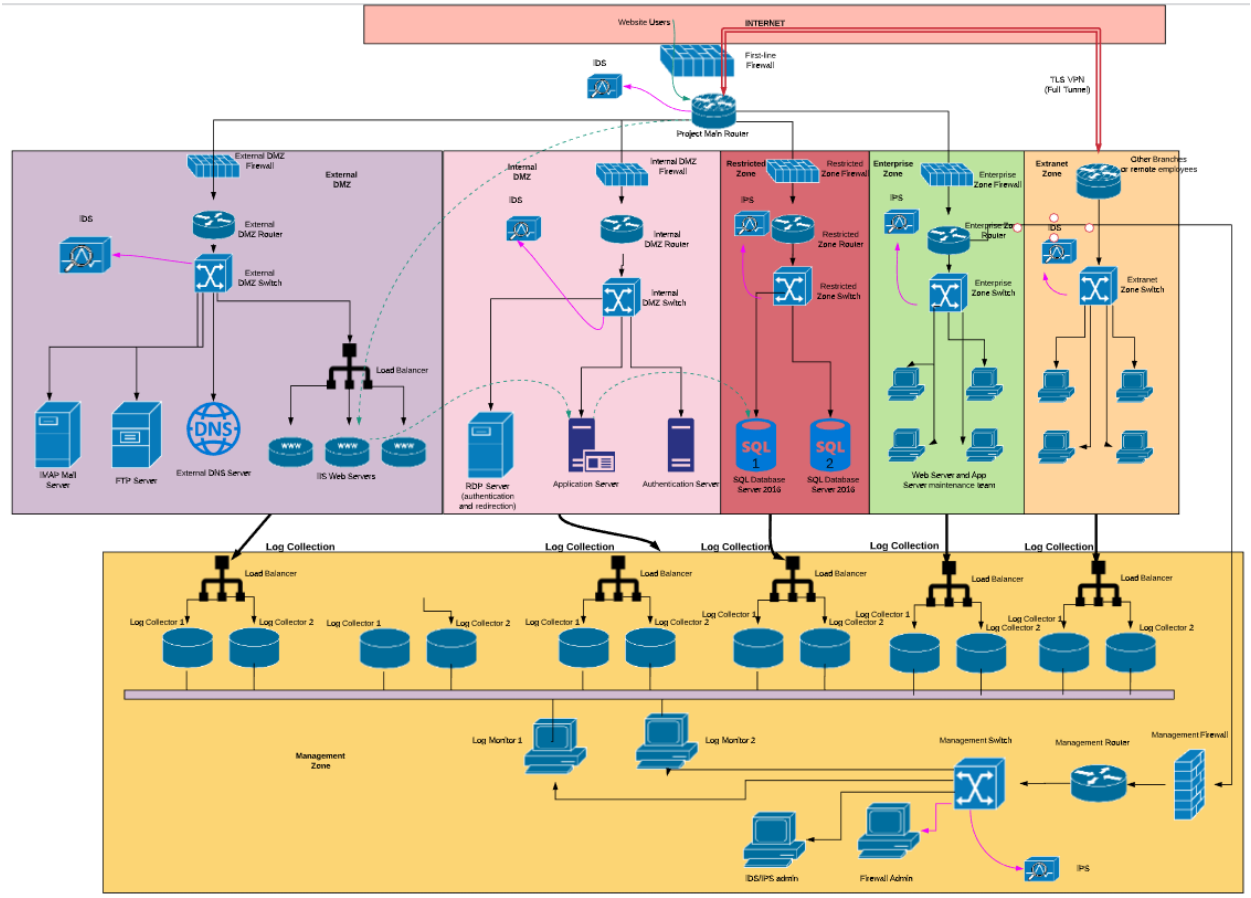


Appendix 3

Detailed Network Topology for HIC

In the case of HIC, the network infrastructure is well-layered and multi-tiered, as it is segmented into 6 zones: External and Internal DMZ, Restricted Zone, Enterprise Zone, Extranet Zone and Management Zone.

In terms of enclave protection, for all incoming traffic and requests from the internet, we have our first-line firewall that has strict access list allowing only traffic on ports that are required for business. For instance, it does not allow any port 80 or 8080 connections, but instead enforces the use of HTTPS and forwards such connections to ports 443. After going through the firewall, traffic goes through the Main Router, responsible for distributing packets to the designated servers in the different zones. Routers are effectively configured to minimize any risk of horizontal attacks (gaining access to restricted and internal zones). In fact, only static IP leases are allowed, and the network is subnetted appropriately to utilize all IPs where there is no need for expansion in the future. Additionally, there is a network-based IDS running adjacent to each Zone Router, which is also a part of second-line firewall. Each zone has its own main router and Zone Firewall placed right before the router providing that extra layer of security for inter-zone communications and data exchange. All the logs generated by each zone are collected into the Management Zone, with the help of load balancers. VPN Tunnels are used for inter-branch connectivity and data transfers. The diagram draws a clear picture of how the network is laid out:



References

Modem Pools: https://www.aliexpress.com/popular/8-port-modem-pool.html

Printers: https://www.bestbuy.com/site/hp-laserjet-pro-m479fdw-wireless-color-all-in-one-laser-printer-white/6348956.p?skuId=6348956&ref=212&loc=1&ref=212&loc=1&ds_rl=1262656&gclid=Cj0KCQjwwuD7BRDBARIsAK_5YhX8U5KQZBHw2nieVxtzrqT1IMZDT5Pau_eyDvz91Sbg9OHfxugSPaoaAgcxEALw_wcB&gclsrc=aw.ds

Routers: https://www.serversupply.com/NETWORKING/SWITCH/24%20PORT/CISCO/C9300-24T-A_304882.htm?gclid=Cj0KCQjwwuD7BRDBARIsAK_5YhV914sDxfs6ARgn0ct98WZXCn5LvKrDKD9LzRAR8UoZOUFtiH1eLAUaAqiOEALw_wcB