Class Project Paper

Abhishek Ningala

Security Risk Management and Assessment (IA5200)

Themis A Papageorge

December 5, 2019

NORTHEASTERN UNIVERSITY 360 HUNTINGTON AVE, BOSTON, MA.

Contents

Part A: Security Risk Management Assessment (based on Assignments 1-4 and mid-term presentation)

I) Executive summary based on the data of the NIST template points 1-15

1. Information System Name / Title

Hypothetical Government Agency (HGA)

2. Information System Categorization

Information System Asset	Impact		
	Confidentiality	Integrity	Availability
Financial Resources	High	High	High
System Components	High	High	High
Personnel Information	High	High	High
Contracting and Procurement Documents	High	High	High
Draft Regulations	High	High	High
Internal Correspondence	High	High	High
Business Documents	High	High	High

The overall value is High.

3. Information System Owner

Name: Dennis R Sterling
Title: Chief Information Officer
Agency: Hypothetical Government Agency (HGA)
Address: 4580 Aspen Court, Boston, MA
Email Address: dennis.s@gmail.com
Phone Number: 617-368-2898

4. Authorizing Official

Name: Sophia C Thompson
Title: Chief Security Officer
Agency: Hypothetical Government Agency (HGA)
Address: 4546 Rainy Day Drive, Boston, MA
Email Address: sophia.t@gmail.com
Phone Number: 617-937-5169

5. Other Designated Contacts

Name: Jean J pears
Title: Information Director
Agency: Hypothetical Government Agency (HGA)
Address: 3905 Aspen Court, Boston, MA
Email Address: Jean.jsp@gmail.com
Phone Number: 617-369-1223

6. Assignment of Security Responsibility

Name: Christopher N Jenn
Title: Chief Information Security Officer
Agency: Hypothetical Government Agency (HGA)
Address: 559 Doctors Drive, Boston, MA
Email Address: jenn.chris@gmail.com
Phone Number: 617-828-1496

7. Information System Operational Status

The status of information system operational status of HGA is operational.

8. Information System type

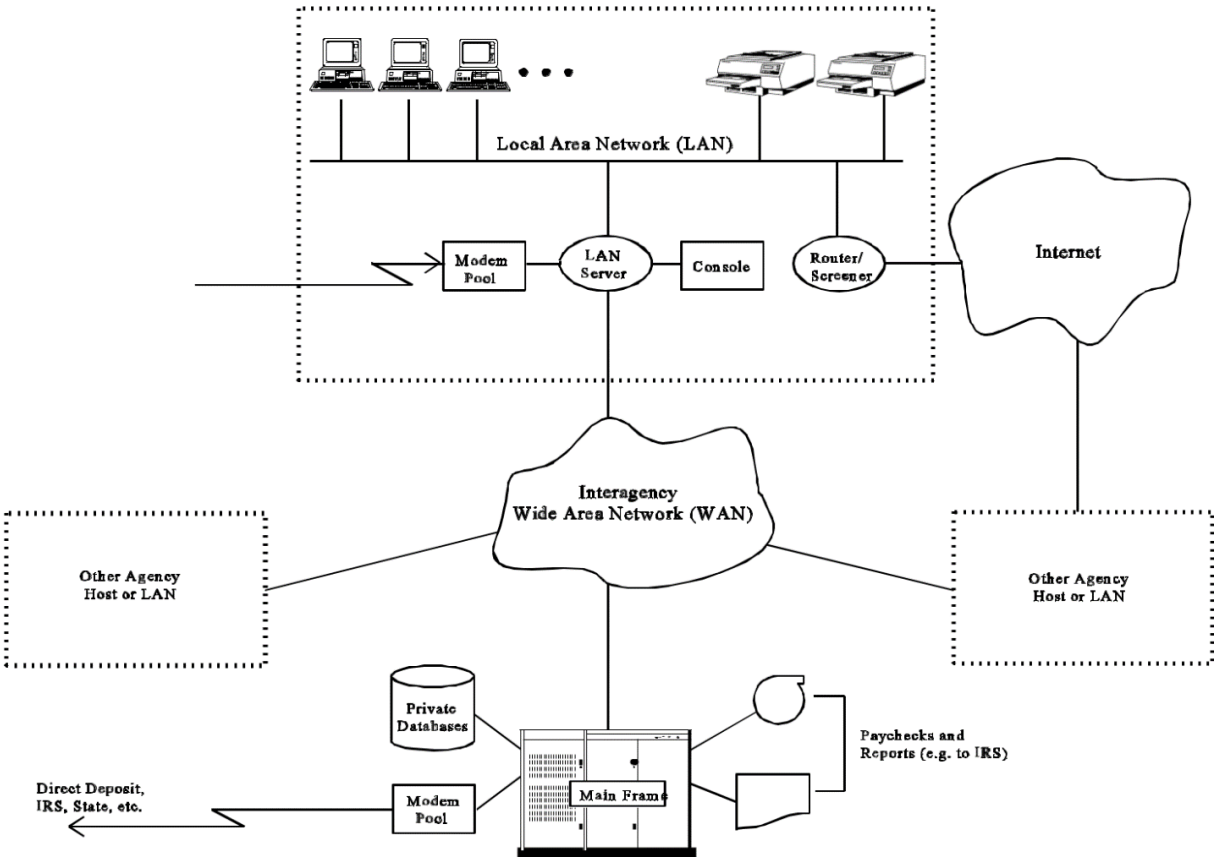
The information system type of HGA is a major application.

9. General System Description / Purpose

HGA's systems play a key role in transferring U.S. Government funds to individuals in the form of paychecks.

10. System Environment

All the PC's in HGA are connected to LAN so that the users can share information among themselves. LAN Server is a central component which also provides a large disk storage for shared information and shared programs. There are several printers distributed throughout the HGA building. LAN provides a connection to the internet via router. A modem pool is provided for dial up connections. A special console is provided for administrative purposes. A WAN is provided so that information can be transferred to or from other agencies.



11. System Interconnections / Information Sharing

System Name: Interagency Wide Network
Organization Type: Telecommunications
Agreement: Government Agency
Date: August 12, 1996
FIPS 199 Category: High
C&A Status: NIST Accredited
Authorizing Official: Sophia C Thompson

System Name: Mainframe
Organization Type: Federal Agency
Agreement: 10-year Contract
Date: May 6, 1990
FIPS 199 Category: High
C&A Status: NIST Accredited
Authorizing Official: Sophia C Thompson

12. Related Laws / Regulations / Policies

There are several Laws, Regulations and Policies that HGA must abide:

- The Computer Fraud and Abuse Act of 1986
- The Computer Security Act of 1997
- Privacy Act
- Gramm–Leach–Bliley
- Sarbanes–Oxley Act
- FIPS-199

13. Minimum Security Controls

Control	Implementation	Status	Control type	Authority responsible
Risk Management(M1)	Risk and security program management themes with risk-driven safeguards	Implemented	Common	CRO
Review of Security Controls(M2)	There are new security controls implemented based on recommendations.	Implemented	Common	CSO
Life Cycle(M3)	System development life cycle implemented	Implemented	Common	CIO
Authorize Processing (M4)	Systems are certified and accredited on regular basis	Implemented	Common	CISO
System Security Plan(M5)	A System Security Plan has been implemented	Implemented	Common	CISO
Personnel Security(O1)	A Security plan for all personnel has been implemented	Implemented	Common	CISO
Physical Security(O2)	Only a few controls for physical security has been implemented	Partially Implemented	Common	CISO
Production, Input/output Controls(O3)	Media and user controls not implemented	Not Implemented	Common	CSO
Contingency Planning(O4)	A comprehensive contingency plan should be developed	Not Implemented	Common	CISO
Hardware and Systems Software Maintenance(O5)	Access controls are limited and have been tested and implemented	Implemented	Common	COG Director

Data Integrity(O6)	Data Integrity checks and tools have to be implemented	Not Implemented	Common	COG Director
Documentation(O7)	Sufficient Documentation has not been provided	Partially Implemented	Common	COG Director
Security Awareness, Training and Education(O8)	Adequate Security training and awareness is provided	Implemented	Common	CISO
Incident Response Capability(O9)	Incident Response Plan is in plan	Implemented	Common	CISO
Identification and Authentication (T1)	Poor Authentication mechanisms are in place.	Partially Implemented	Common	CSO
Logical Access Control (T2)	Sufficient Logical Access control mechanisms are in place	Implemented	Common	CISO
Audit Trails (T3)	Audit logging capabilities are not in place	Not Implemented	Common	CSO

14. Information System Security Plan Completion Date

October 6, 2019

15. Information System Security Plan Approval Date

October 7, 2019

II. List of Assets with Values

Hypothetical government agency (HGA) has information systems that comprise of different kind of assets which includes financial resources, personnel information, contracting and procurement documents etc. which needs protection. HGA employs 500 personnel. The company has a total of 600 PCs, 50 Printers, 30 modem pools, 10 LAN servers, 20 consoles, and 40 routers. The average cost of each component is as follows:

- PC - $600
- LAN Server - $4000
- Printer - $200
- Model Pool - $200
- Console - $2000
- Router - $400

- **Information Assets inventory**

No.	Asset	Value
A1	Financial Resources	$25,000,000
A2	System Components	$472,000
A21	PC's	$360,000
A22	LAN Server	$40,000
A23	Printers	$10,000
A24	Modem Pool	$6000
A25	Console	$40,000
A26	Router	$16,000
A3	Personnel Information	$5,000,000
A4	Contracting and Procurement Documents	$2,000,000
A5	Draft Regulations	$100,000
A6	Internal Correspondence	$500,000
A7	Business Documents	$2,000,000
A8	Reputation	Intangible
A9	Employee Confidence	Intangible

- **Subset of Assets:**

No.	Assets	Asset value
A1	Financial Resources	$25,000,000
A22	LAN Server	$40,000
A26	Router	$16,000
A3	Personnel Information	$5,000,000

III. List of Threats

- **List of Threats:**

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

- **Selection of subset of threats:**

No.	Threats
T1	Payroll Fraud
T2	Payroll Errors
T4	Disclosure or Brokerage of Information
T5	Network-Related Attacks

IV. List of Vulnerabilities

- **List of Security Vulnerabilities:**

No.	Vulnerabilities
T1:V1	Vulnerabilities related to payroll fraud
V1.1	Falsified Time Sheets
V1.2	Unauthorized Access
V1.3	Bogus Time and Attendance Applications
V1.4	Unauthorized Modifications of Time and Attendance Sheets
T2:V2	Vulnerabilities Related to Payroll Errors
T3:V3	Vulnerabilities Related to Continuity of Operations
V3.1	COG Contingency Planning
V3.2	Division Contingency Planning
V3.3	Virus Prevention
V3.4	Accidental Corruption and Loss of Data
T4:V4	Vulnerabilities Related to Disclosure or Brokerage of information
T5:V5	Vulnerabilities Related to Network-Related Attacks

- **Selection of subset of vulnerabilities:**

No.	Vulnerabilities
V1.2	Unauthorized Access
V3.4	Accidental Corruption and Loss of Data
V4	Vulnerabilities Related to Disclosure or Brokerage of information
V5	Vulnerabilities Related to Network-Related Attacks

V. Threat / Vulnerability Pairs

- **List of threat vulnerability pairs:**

Vulnerabilities/Threats	T1	T2	T3	T4
V1.2 on A1,A22,A26,A3	80%	30%	60%	50%
V3.4 on A1,A22,A26,A3	30%	60%	20%	50%
V4 on A1,A22,A26,A3	20%	10%	80%	30%
V5 on A1,A22,A26,A3	40%	20%	50%	80%

VI. Assets Impacted by Threat / Vulnerability Pairs

- **List of assets impacted by Threat / vulnerability pairs**

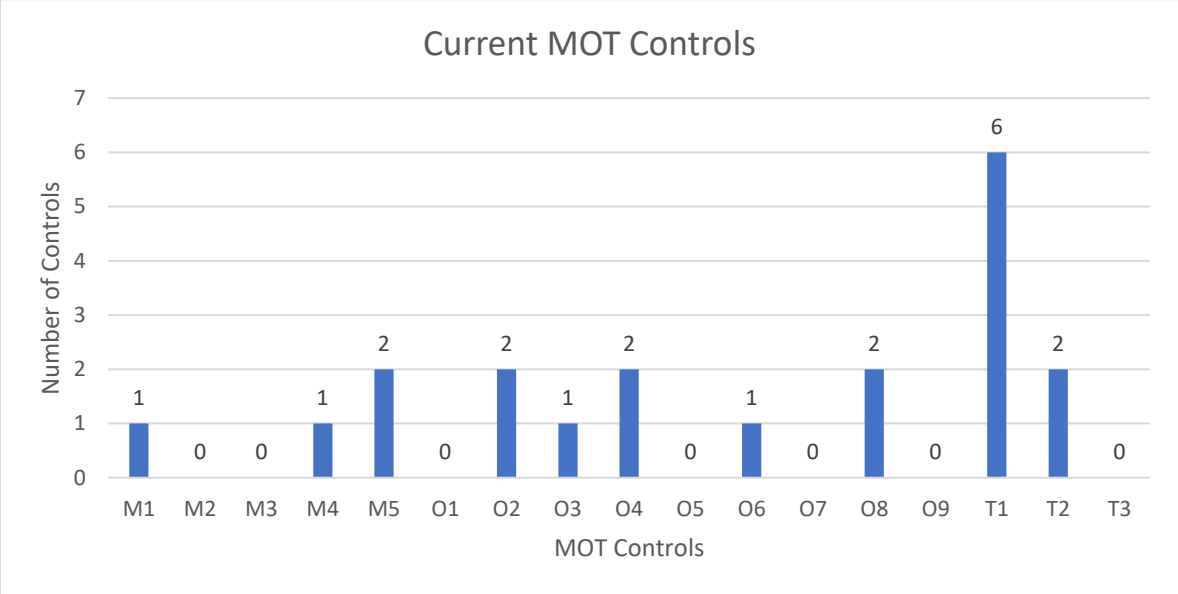
Asset	Vulnerability
A1: Financial Resources	Unauthorized Access
	Accidental Corruption and Loss of Data
	Vulnerabilities Related to Disclosure or Brokerage of information
	Vulnerabilities Related to Network-Related Attacks
A2: LAN Server	Unauthorized Access
	Accidental Corruption and Loss of Data
	Vulnerabilities Related to Disclosure or Brokerage of information
	Vulnerabilities Related to Network-Related Attacks

Asset	Vulnerability
A3: Router	Unauthorized Access
	Accidental Corruption and Loss of Data
	Vulnerabilities Related to Disclosure or Brokerage of information
	Vulnerabilities Related to Network-Related Attacks
A4: Personnel Information	Unauthorized Access
	Accidental Corruption and Loss of Data
	Vulnerabilities Related to Disclosure or Brokerage of information
	Vulnerabilities Related to Network-Related Attacks

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

Management	Operational	Technical
Risk Management (M1)	Personnel Security (O1)	Identification and Authentication (T1)
Review of Security Controls (M2)	Physical Security (O2)	Logical Access Control (T2)
Life Cycle (M3)	Production, Input/output Controls (O3)	Audit Trails (T3)
Authorize Processing (M4)	Contingency Planning (O4)	
System Security Plan (M5)	Hardware and Systems Software and Maintenance (O5)	
	Data Integrity (O6)	
	Documentation (O7)	
	Security Awareness, Training and Education (O8)	
	Incident Response Capability (O9)	

No.	Security Controls	MOT
C1	General Use and Administrative Controls	
C1.1	Login IDs and Passwords	T1
C1.2	Written Authorization	T1
C1.3	Training and Awareness Session	O8,M5
C1.4	Acknowledgement Forms	T1
C2	Protection Against Payroll Fraud and Errors	
C2.1	Protection Against Unauthorized Execution	T1
C2.2	Protection Against Payroll Errors	T2
C2.3	Protection Against Accidental Corruption or Loss of Payroll Data	O6
C3	Protection Against Interruption of Operations	
C3.1	COG Contingency Planning	O4
C3.2	Division Contingency Planning	O4
C4	Protection Against Disclosure or Brokerage of Information	
C4.1	Secure Storage	O2,O3
C4.2	HGA PC Lock	O2
C4.3	LAN Access Controls	T2
C4.4	Security Awareness Training	O8
C5	Protection Against Network-Related Threats	T1,M1,M5
C6	Protection Against Risks from Non–HGA Computer Systems	T1,M4

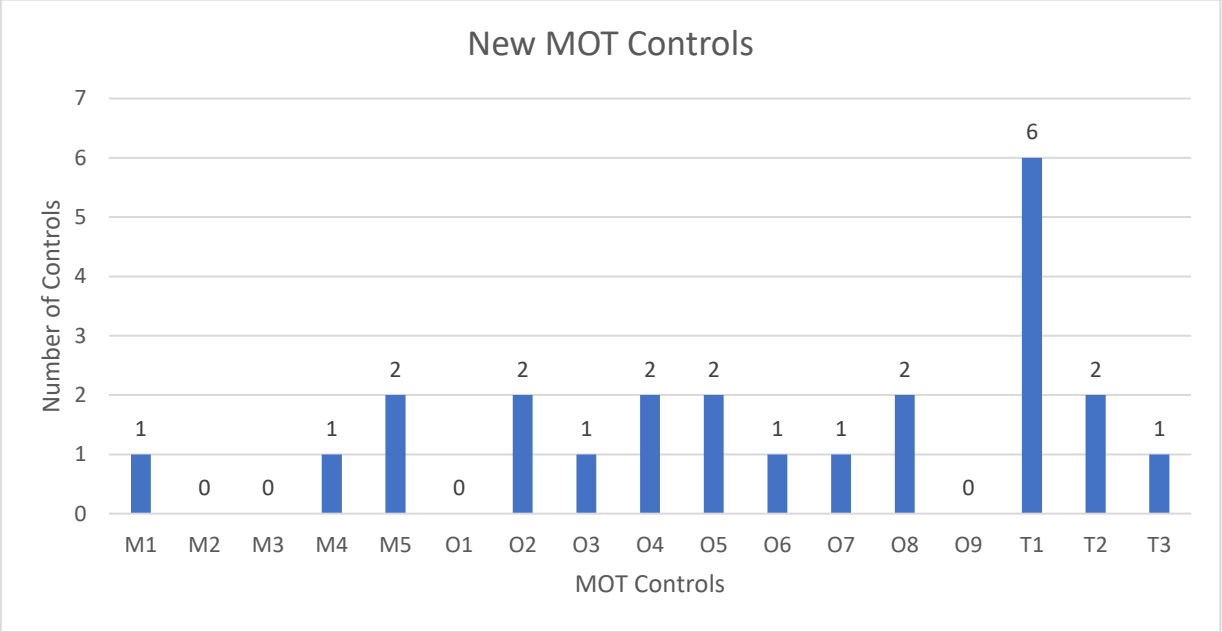


VIII. MOT – which MOT controls are covered by current AND proposed by new CISO HGA controls AND VPN server AND DMZ (Histogram)

No.	New Controls	MOT
NC1	Controls Mitigating Vulnerabilities Related to Payroll Fraud	
NC1.1	Server Administrative procedures and bug-fixes	O5,O3
NC1.2	One-time passwords	T1
NC1.3	Digital signatures	T1
NC2	Controls Mitigating Payroll Error	T3
NC3	Controls Mitigating Vulnerabilities Related to Continuity of Operations	
NC3.1	SETA	O8
NC3.2	Mainframe MOU	O7,O4
NC3.3	Automated E-mail Reminders and Back-ups	O5,O4
NC4	Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of information	
NC4.1	Screen locks	T1,O2
NC4.2	Hard Disk Encryption	O2
NC5	Controls Vulnerabilities Related to Network-Related Attacks	
NC5.1	Stronger I&A	T1,,T2,O8
NC5.2	Encrypting modems	M1
NC5.3	Mainframe Communications Encryption	M1,M4

Values for VPN – M5, O6, T1,

Values for DMZ – M5, T2,T1



IX. Security Risk Prevention Strategy 1

Security Risk ($) Calculations of Assets with vulnerabilities discovered by new CISO and protected by current controls. Calculate residual risks for assets and total HGA residual risk. Calculate vulnerability risks for ranking which vulnerability should be addressed by controls first, second, third etc.

List of Information Assets Inventory:

No.	Assets	Asset value
A1	Financial Resources	$25,000,000
A22	LAN Server	$40,000
A26	Router	$16,000
A3	Personnel Information	$5,000,000

Threat Vulnerability matrix with probability of exploitation

Vulnerabilities/Threats	T1	T2	T3	T4
V1.2 on A1,A22,A26,A3	40%	8%	30%	20%
V3.4 on A1,A22,A26,A3	10%	40%	80%	30%
V4 on A1,A22,A26,A3	8%	8%	30%	10%
V5 on A1,A22,A26,A3	6%	6%	10%	30%

Initial Risk Impacts:

If a threat exploits a vulnerability, we assume that the risk impact would be 100% or the resilience would be 0%.

	T1*V1.2	T1*V3.4	T1*V4	T1*V5	T2*V1.2	T2*V3.4	T2*V4	T2*V5	T3*V1.2	T3*V3.4	T3*V4	T3*V5	T4*V1.2	T4*V3.4	T4*V4	T4*V5
A1-100	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A22-85	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A26-90	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A3-95	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Risk Calculations:

- **Risk of A1:**
  $25,000,000*(40%+8%+30%+20%+10%+40%+80%+30%+8%+8%+30%+10%+6%+6%+10%+30%) = $91,500,000> $25,000,000, therefore Risk of A1= $25,000,000 (total asset loss)
- **Risk of A22:**
  $40,000*(40%+8%+30%+20%+10%+40%+80%+30%+8%+8%+30%+10%+6%+6%+10%+30%) = $146,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)
- **Risk of A26:**
  $16,000*(40%+8%+30%+20%+10%+40%+80%+30%+8%+8%+30%+10%+6%+6%+10%+30%) = $58560> $16,000, therefore Risk of A26= $16,000 (total asset loss)
- **Risk of A3:**
  $5,000,000*(40%+8%+30%+20%+10%+40%+80%+30%+8%+8%+30%+10%+6%+6%+10%+30%) = $183,00,000> $5,000,000, therefore Risk of A3= $5,000,000 (total asset loss)

  Thus, residual risk of all assets is $30,056,000.

- **Risk due to V1.2:** $25,000,000*(40%+8%+30%+20%) + $40,000*(40%+8%+30%+20%) + $16,000*(40%+8%+30%+20%) + $5,000,000*(40%+8%+30%+20%) = $29,454,880
- **Risk due to V3.4:** $25,000,000*(10%+40%+80%+30%) + $40,000*(10%+40%+80%+30%) + $16,000*(10%+40%+80%+30%) + $5,000,000*(10%+40%+80%+30%) = $48,089,600
- **Risk due to V4:** $25,000,000*(8%+8%+30%+10%) + $40,000*(8%+8%+30%+10%) + $16,000*(8%+8%+30%+10%) + $5,000,000*(8%+8%+30%+10%) = $16,831,360
- **Risk due to V5:** $25,000,000*(6%+6%+10%+30%) + $40,000*(6%+6%+10%+30%) + $16,000*(6%+6%+10%+30%)+ $5,000,000*(6%+6%+10%+30%) = 15,029,120

Ranking of security asset residual risks:

Rank	Asset
1	A1: Financial Resources
2	A3: Personnel Information
3	A22: LAN Server
4	A26: Router

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V3.4: Accidental Corruption and Loss of Data
2	V1.2: Unauthorized Access
3	V4: Vulnerabilities Related to Disclosure or Brokerage of information
4	V5: Vulnerabilities Related to Network-Related Attacks

X. Security Risk Prevention Strategy 2

Security Risk ($) Calculations of Assets with vulnerabilities discovered by new CISO and protected by current and proposed by new CISO controls. Calculate residual risks for assets and total HGA residual risk. Calculate vulnerability risks for ranking of which vulnerability should be addressed by controls first, second, third etc.

The highest ranked vulnerability in my case is V3.4: Accidental Corruption and loss of data. Data backups are a good way to safeguard against data loss. As the data is important, it is necessary to store the data at multiple offsite locations.

Updated Threat/Vulnerability pairs with further reduced probabilities:

Vulnerabilities/Threats	T1	T2	T3	T4
V1.2 on A1,A22,A26,A3	40%	8%	30%	20%
V3.4 on A1,A22,A26,A3	8%	20%	40%	20%
V4 on A1,A22,A26,A3	8%	8%	30%	10%
V5 on A1,A22,A26,A3	6%	6%	10%	30%

Initial Risk Impacts:

If a threat exploits a vulnerability, we assume that the risk impact would be 100% or the resilience would be 0%.

	T1*V1.2	T1*V3.4	T1*V4	T1*V5	T2*V1.2	T2*V3.4	T2*V4	T2*V5	T3*V1.2	T3*V3.4	T3*V4	T3*V5	T4*V1.2	T4*V3.4	T4*V4	T4*V5
A1-100	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A22-85	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A26-90	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A3-95	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Risk Calculations:

Risk on A1:
100*(40%+8%+30%+20%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 294 > 100, therefore Risk of A1 = 100 (total asset loss)

Risk on A22:

85*(40%+8%+30%+20%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 249.9 > 85, therefore Risk of A22 = 85 (total asset loss)

Risk on A26:

90*(40%+8%+30%+20%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 264.6 > 90, therefore Risk of A26 = 90 (total asset loss)

Risk on A3:

95*(40%+8%+30%+20%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 279.3 > 95, therefore Risk of A3 = 95 (total asset loss)

Thus, Residual risk of all assets is 370.

Risk due to V1.2: 100*(40%+8%+30%+20%) + 85*(40%+8%+30%+20%) + 90*(40%+8%+30%+20%) + 95*(40%+8%+30%+20%) = 362.6

Risk due to V3.4: 100*(8%+20%+40%+20%) + 85*(8%+20%+40%+20%) + 90*(8%+20%+40%+20%) + 95*(8%+20%+40%+20%) = 325.6

Risk due to V4: 100*(8%+8%+30%+10%) + 85*(8%+8%+30%+10%) + 90*(8%+8%+30%+10%) + 95*(8%+8%+30%+10%) = 207.2

Risk due to V5: 100*(6%+6%+10%+30%) + 85*(6%+6%+10%+30%) + 90*(6%+6%+10%+30%) + 95*(6%+6%+10%+30%) = 192.4

Ranking of security asset residual risks:

Rank	Asset
1	A1: Financial Resources
2	A3: Personnel Information
3	A26: Router
4	A22: LAN Server

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V1.2: Unauthorized Access
2	V3.4: Accidental Corruption and Loss of Data
3	V4: Vulnerabilities Related to Disclosure or Brokerage of information
4	V5: Vulnerabilities Related to Network-Related Attacks

XI. Security Risk Prevention Strategy 3

Security Risk ($) Calculations of Assets with vulnerabilities discovered by new CISO and protected by current and proposed by new CISO controls and non-covered/missing MOT controls. Calculate residual risks for assets and total HGA residual risk. Calculate vulnerability risks for ranking which vulnerability should be addressed by controls first, second, third etc. Compare HGA current, CISO proposed, and VPN and DMZ risk controls to the 157 risk controls from Common Criteria.

Missing M-O-T Controls:

- **Cryptography** (No hard disk encryption)
- **Audit Trails** (No Activity logs)
- **Security considerations**
- **Assurance**

Now, the highest ranked vulnerability risk is V1.2: Unauthorized access. Upgrading to use of one-time passwords for time and attendance sessions on the server. Also, digital signatures on the mainframes based on public key cryptography can be employed to detect unauthorized modification of time and attendance data.

- **Updated Threat/Vulnerability pairs with further reduced probabilities:**

Vulnerabilities/Threats	T1	T2	T3	T4
V1.2 on A1,A22,A26,A3	30%	6%	20%	10%
V3.4 on A1,A22,A26,A3	8%	20%	40%	20%
V4 on A1,A22,A26,A3	8%	8%	30%	10%
V5 on A1,A22,A26,A3	6%	6%	10%	30%

- **Initial Risk Impacts:**

If a threat exploits a vulnerability, we assume that the risk impact would be 100% or the resilience would be 0%.

	T1*V1.2	T1*V3.4	T1*V4	T1*V5	T2*V1.2	T2*V3.4	T2*V4	T2*V5	T3*V1.2	T3*V3.4	T3*V4	T3*V5	T4*V1.2	T4*V3.4	T4*V4	T4*V5
A1-100	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A22-85	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A26-90	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

A3-95	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Risk Calculations:

- **Risk on A1:**
  100*(30%+6%+20%+10%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 262 > 100, therefore Risk of A1 = 100 (total asset loss)
- **Risk on A22:**
- 85*(30%+6%+20%+10%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 222.7 > 85, therefore Risk of A22 = 85 (total asset loss)
- **Risk on A26:**
- 90*(30%+6%+20%+10%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 235.8 > 90, therefore Risk of A26 = 90 (total asset loss)
- **Risk on A3:**
- 95*(30%+6%+20%+10%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 248.9 > 95, therefore Risk of A3 = 95 (total asset loss)

Thus, Residual risk of all assets is 370.

- **Risk due to V1.2:** 100*(30%+6%+20%+10%) + 85*(30%+6%+20%+10%) + 90*(30%+6%+20%+10%) + 95*(30%+6%+20%+10%) = 244.2
- **Risk due to V3.4:** 100*(8%+20%+40%+20%) + 85*(8%+20%+40%+20%) + 90*(8%+20%+40%+20%) + 95*(8%+20%+40%+20%) = 325.6
- **Risk due to V4:** 100*(8%+8%+30%+10%) + 85*(8%+8%+30%+10%) + 90*(8%+8%+30%+10%) + 95*(8%+8%+30%+10%) = 207.2
- **Risk due to V5:** 100*(6%+6%+10%+30%) + 85*(6%+6%+10%+30%) + 90*(6%+6%+10%+30%) + 95*(6%+6%+10%+30%) = 192.4

Ranking of security asset residual risks:

Rank	Asset
1	A1: Financial Resources
2	A3: Personnel Information
3	A26: Router
4	A22: LAN Server

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V3.4: Accidental Corruption and Loss of Data
2	V1.2: Unauthorized Access
3	V4: Vulnerabilities Related to Disclosure or Brokerage of information
4	V5: Vulnerabilities Related to Network-Related Attacks

Compare HGA current, CISO proposed, and VPN and DMZ risk controls to the 157 risk controls from Common Criteria

After the initial risk assessment, new controls were proposed by the new CISO's team. The HGA management have successfully implemented most of the controls from the Common Criteria. However, they were a few controls left out like the physical and environmental security controls which are yet to be implemented. VPN and DMZ were implemented to harden the security controls of the HGA. Some of the missing MOT controls are:

- Cryptography (No hard disk encryption)
- Audit Trails (No Activity logs)
- Security considerations
- Assurance

Some of the controls which have been implemented by following the Common Criteria are:

- Cryptography (encryption)
- Media Access Protection

XII. Security Risk Prevention Strategy and Security Risk Response (Resilience) Strategy

Apply Hardening Controls to highest ranked Residual Asset Risk, thus reducing Risk Impact probabilities, and further reducing the overall security asset residual risk. Calculate residual risks for assets and total HGA residual risk. Provide a ranking for which vulnerability should be addressed by controls first, second, third etc. and a ranking for which risk impact should be addressed by controls first, second, third etc. Compare HGA current, CISO proposed, and VPN and DMZ risk controls to the 157 risk controls from Common Criteria.

❖ **Security Risk Prevention Strategy:**

- **Information Assets inventory**

No.	Asset	Value
A1	Financial Resources	$25,000,000
A2	System Components	$472,000
A21	PC's	$360,000
A22	LAN Server	$40,000
A23	Printers	$10,000
A24	Modem Pool	$6000
A25	Console	$40,000
A26	Router	$16,000
A3	Personnel Information	$5,000,000
A4	Contracting and Procurement Documents	$2,000,000
A5	Draft Regulations	$100,000
A6	Internal Correspondence	$500,000
A7	Business Documents	$2,000,000
A8	Reputation	Intangible
A9	Employee Confidence	Intangible

List of Information Assets Inventory:

No.	Assets	Asset value
A1	Financial Resources	$25,000,000
A22	LAN Server	$40,000
A24	VPN Server	$6000
A26	Router	$16,000
A3	DMZ	$50,000
A4	Personnel Information	$5,000,000

Threat Vulnerability Pairs

Vulnerabilities/Threats	T1	T2	T3	T4	T5
V1.2 on A1,A22,A24,A26,A3,A4	40%	8%	30%	20%	10%
V1.4 on A1,A22,A24,A26,A3,A4	20%	10%	30%	10%	20%
V3.4 on A1,A22,A24,A26,A3,A4	10%	40%	80%	30%	10%
V4 on A1,A22,A24,A26,A3,A4	8%	8%	30%	10%	30%
V5 on A1,A22,A24,A26,A3,A4	6%	6%	10%	30%	10%

Calculations:

Risk of A1:
$25,000,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $129,000,000> $25,000,000, therefore Risk of A1= $25,000,000 (total asset loss)

Risk of A22:
$40,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $206,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)

Risk of A24:

$6000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $30960> $16,000, therefore Risk of A24= $6,000 (total asset loss)

Risk of A26:
$16,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $82560> $16,000, therefore Risk of A26= $16,000 (total asset loss)

Risk of A3:

$50,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $258,000> $50,000, therefore Risk of A3= $50,000 (total asset loss)

Risk of A4:
$5,000,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8

%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $258,00,000> $5,000,000, therefore Risk of A3= $5,000,000 (total asset loss)

Thus, residual risk of all assets is $30,112,000.

Risk due to V1.2: $25,000,000*(40%+8%+30%+20%+10%) + $40,000*(40%+8%+30%+20%+10%) + $6,000*(40%+8%+30%+20%+10%) + $16,000*(40%+8%+30%+20%+10%) + $50,000*(40%+8%+30%+20%+10%) + $5,000,000*(40%+8%+30%+20%+10%) = $32,520,960

Risk due to V1.4: $25,000,000*(20%+10%+30%+10%+20%) + $40,000*(20%+10%+30%+10%+20%) + $6,000*(20%+10%+30%+10%+20%) + $16,000*(20%+10%+30%+10%+20%) + $50,000*(20%+10%+30%+10%+20%) + $5,000,000*(20%+10%+30%+10%+20%) = $27,100,800

Risk due to V3.4: $25,000,000*(10%+40%+80%+30%+10%) + $40,000*(10%+40%+80%+30%+10%) + $6,000*(10%+40%+80%+30%+10%) + $16,000*(10%+40%+80%+30%+10%) + $50,000*(10%+40%+80%+30%+10%) + $5,000,000*(10%+40%+80%+30%+10%) = $51,190,400

Risk due to V4: $25,000,000*(8%+8%+30%+10%+30%) + $40,000*(8%+8%+30%+10%+30%) + $6,000*(8%+8%+30%+10%+30%) + $16,000*(8%+8%+30%+10%+30%) + $50,000*(8%+8%+30%+10%+30%) + $5,000,000*(8%+8%+30%+10%+30%) = $25,896,320

Risk due to V5: $25,000,000*(6%+6%+10%+30%+10%) + $40,000*(6%+6%+10%+30%+10%) +$6,000*(6%+6%+10%+30%+10%) + $16,000*(6%+6%+10%+30%+10%) + $50,000*(6%+6%+10%+30%+10%) + $5,000,000*(6%+6%+10%+30%+10%) = 18,669,440

Ranking of security asset residual risks:

Rank	Asset
1	A1: Financial Resources
2	A4: Personnel Information
3	A3: DMZ
4	A22: LAN Server
5	A26: Router
6	A24: VPN Server

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V3.4: Accidental Corruption and Loss of Data
2	V1.2: Unauthorized Access
3	V1.4: Unauthorized Modification of time and Attendance sheets
4	V4: Vulnerabilities Related to Disclosure or Brokerage of information
5	V5: Vulnerabilities Related to Network-Related Attacks

❖ **Security Risk Response Strategy:**

No.	Assets	Asset value
A1	Financial Resources	$25,000,000
A22	LAN Server	$40,000
A24	VPN Server	$6000
A25	Console	$40,000
A26	Router	$16,000
A3	DMZ	$50,000
A4	Personnel Information	$5,000,000

Threat/Vulnerability pairs with further reduced probabilities:

Vulnerabilities/Threats	T1	T2	T3	T4	T5
V1.2 on A1,A22,A24,A26,A3,A4	40%	8%	30%	20%	10%
V1.4 on A1,A22,A24,A26,A3,A4	20%	10%	30%	10%	20%
V3.4 on A1,A22,A24,A26,A3,A4	10%	40%	80%	30%	10%
V4 on A1,A22,A24,A26,A3,A4	8%	8%	30%	10%	30%
V5 on A1,A22,A24,A26,A3,A4	6%	6%	10%	30%	10%

The highest ranked Residual Asset Risk is the A1: Financial Resources. We now apply hardening controls to reduce the residual risk of financial resources.

	T1*V1.2	T1*V1.4	T1*V3.4	T1*V4	T1*V5	T2*V1.2	T2*V1.4	T2*V3.4	T2*V4	T2*V5	T3*V1.2	T3*V1.4	T3*V3.4	T3*V4	T3*V5	T4*V1.2	T4*V1.4	T4*V3.4	T4*V4	T4*V5	T5*V1.2	T5*V1.4	T5*V3.4	T5*V4	T5*V5
A1	80%	60%	70%	90%	60%	90%	70%	60%	80%	70%	90%	80%	60%	70%	80%	60%	70%	90%	80%	70%	60%	90%	80%	70%	60%
A22	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%
A26	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%	100%
A4	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%	100%

Risk Calculations:

Risk of A1:
25,000,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%+20%*60%+10%*70%+30%*80%+10%*70%+20%*90%+10%*70%+40%*60%+80%*60%+30%*90%+10%*80%+8%*90%+8%*80%+30%*70%+10%*80%+30%*70%+6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) = $15,165,000<$25,000,000, therefore Risk of A1 = $15,165,000 (partial asset loss)

Risk of A22:
$40,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $206,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)

Risk of A24:

$6000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $30,960> $6,000, therefore Risk of A24= $6,000 (total asset loss)

Risk of A25:
$40,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $206,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)

Risk of A26:
$16,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $82,560> $16,000, therefore Risk of A26= $16,000 (total asset loss)

Risk of A3:

$50,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $258,000> $50,000, therefore Risk of A3= $50,000 (total asset loss)

Risk of A4:
$5,000,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $25,800,000> $5,000,000, therefore Risk of A3= $5,000,000 (total asset loss)

Thus, residual risk of all assets is $20,317,000.

Risk due to V1.2: $25,000,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%) + $40,000*(40%+8%+30%+20%+10%) + $6,000*(40%+8%+30%+20%+10%) + $40,000*(40%+8%+30%+20%+10%) $16,000*(40%+8%+30%+20%+10%) + $50,000*(40%+8%+30%+20%+10%) + $5,000,000*(40%+8%+30%+20%+10%) = $32,520,960

Risk due to V1.4: $25,000,000*(20%*60%+10%*70%+30%*80%+10%*70%+20%*90%) + $40,000*(20%+10%+30%+10%+20%) + $6,000*(20%+10%+30%+10%+20%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(20%+10%+30%+10%+20%) + $50,000*(20%+10%+30%+10%+20%) + $5,000,000*(20%+10%+30%+10%+20%) = $21,636,800

Risk due to V3.4: $25,000,000*(10%*70%+40%*60%+80%*60%+30%*90%+10%*80%) + $40,000*(10%+40%+80%+30%+10%) + $6,000*(10%+40%+80%+30%+10%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(10%+40%+80%+30%+10%) + $50,000*(10%+40%+80%+30%+10%) + $5,000,000*(10%+40%+80%+30%+10%) = $37,258,400

Risk due to V4: $25,000,000*(8%*90%+8%*80%+30%*70%+10%*80%+30%*70%) + $40,000*(8%+8%+30%+10%+30%) + $6,000*(8%+8%+30%+10%+30%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(8%+8%+30%+10%+30%) + $50,000*(8%+8%+30%+10%+30%) + $5,000,000*(8%+8%+30%+10%+30%) = $20,330,720

Risk due to V5: $25,000,000*(6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) + $40,000*(6%+6%+10%+30%+10%) +$6,000*(6%+6%+10%+30%+10%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(6%+6%+10%+30%+10%) + $50,000*(6%+6%+10%+30%+10%) + $5,000,000*(6%+6%+10%+30%+10%) = 13,894,240

Ranking of security asset residual risks: Ranking of security asset residual risks:

Rank	Asset	Value
1	A4: Personnel Information	$5,000,000
2	A1: Financial Resources	$15,165,000
3	A3: DMZ	$50,000
4	A22: LAN Server	$40,000
5	A25: Console	$40,000
6	A26: Router	$16,000
7	A24: VPN Server	$6000

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V3.4: Accidental Corruption and Loss of Data
2	V1.2: Unauthorized Access
3	V1.4: Unauthorized Modification of time and Attendance sheets
4	V4: Vulnerabilities Related to Disclosure or Brokerage of information
5	V5: Vulnerabilities Related to Network-Related Attacks

- **Mixed Strategy:**

The highest ranked Residual Asset now is the A4: Personnel Information. We now apply hardening controls to reduce the residual risk of this asset.

Threat/Vulnerability pairs with further reduced probabilities:

Vulnerabilities/Threats	T1	T2	T3	T4	T5
V1.2 on A1,A22,A24,A26,A3,A4	40%	8%	30%	20%	10%
V1.4 on A1,A22,A24,A26,A3,A4	20%	10%	30%	10%	20%
V3.4 on A1,A22,A24,A26,A3,A4	10%	40%	80%	30%	10%
V4 on A1,A22,A24,A26,A3,A4	8%	8%	30%	10%	30%
V5 on A1,A22,A24,A26,A3,A4	6%	6%	10%	30%	10%

Risk Matrix:

	T1*V1.2	T1*V1.4	T1*V3.4	T1*V4	T1*V5	T2*V1.2	T2*V1.4	T2*V3.4	T2*V4	T2*V5	T3*V1.2	T3*V1.4	T3*V3.4	T3*V4	T3*V5	T4*V1.2	T4*V1.4	T4*V3.4	T4*V4	T4*V5	T5*V1.2	T5*V1.4	T5*V3.4	T5*V4	T5*V5
A1	80%	60%	70%	90%	60%	90%	70%	60%	80%	70%	90%	80%	60%	70%	80%	60%	70%	90%	80%	70%	60%	90%	80%	70%	60%
A22	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%	100%
A26	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%	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%	100%
A4	80%	60%	70%	90%	60%	90%	70%	60%	80%	70%	90%	80%	60%	70%	80%	60%	70%	90%	80%	70%	60%	90%	80%	70%	60%	

Risk Calculations:

Risk of A1:
15,165,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%+20%*60%+10%*70%+30%*80%+10%*70%+20%*90%+10%+70%+40%*60%+80%*60%+30%*90%+10%+80%+8%*90%+8%*80%+30%*70%+10%*80%+30%+70%+6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) = 9,199,089<15,165,000, therefore Risk of A1 = $9,199,089 (partial asset loss)

Risk of A22:
$40,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $206,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)

Risk of A24:

$6000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $30,960> $6,000, therefore Risk of A24= $6,000 (total asset loss)

Risk of A25:
$40,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $206,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)

Risk of A26:
$16,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $82,560> $16,000, therefore Risk of A26= $16,000 (total asset loss)

Risk of A3:

$50,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $258,000> $50,000, therefore Risk of A3= $50,000 (total asset loss)

Risk of A4:
$5,000,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%+20%*60%+10%*70%+30%*80%+10%*70%+20%*90%+10%+70%+40%*60%+80%*60%+30%*90%+10%+80%+8%*90%+8%*80%+30%*70%+10%*80%+30%+70%+6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) = $3,033,000< $5,000,000, therefore Risk of A3= $3,033,000 (partial asset loss)

Thus, residual risk of all assets is $12,384,089

Risk due to V1.2: $15,165,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%) + $40,000*(40%+8%+30%+20%+10%) + $6,000*(40%+8%+30%+20%+10%) + $40,000*(40%+8%+30%+20%+10%) $16,000*(40%+8%+30%+20%+10%) + $50,000*(40%+8%+30%+20%+10%) + $3,033,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%) = $15,486,876

Risk due to V1.4: $15,165,000*(20%*60%+10%*70%+30%*80%+10%*70%+20%*90%) + $40,000*(20%+10%+30%+10%+20%) + $6,000*(20%+10%+30%+10%+20%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(20%+10%+30%+10%+20%) + $50,000*(20%+10%+30%+10%+20%) + $3,033,000*(20%*60%+10%*70%+30%*80%+10%*70%+20%*90%) = $12,511,440

Risk due to V3.4: $15,165,000*(10%*70%+40%*60%+80%*60%+30%*90%+10%*80%) + $40,000*(10%+40%+80%+30%+10%) + $6,000*(10%+40%+80%+30%+10%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(10%+40%+80%+30%+10%) + $50,000*(10%+40%+80%+30%+10%) + $3,033,000*(10%*70%+40%*60%+80%*60%+30%*90%+10%*80%) = $21,004,120

Risk due to V4: $15,165,000*(8%*90%+8%*80%+30%*70%+10%*80%+30%*70%) + $40,000*(8%+8%+30%+10%+30%) + $6,000*(8%+8%+30%+10%+30%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(8%+8%+30%+10%+30%) + $50,000*(8%+8%+30%+10%+30%) + $3,033,000*(8%*90%+8%*80%+30%*70%+10%*80%+30%*70%) = $11,704,648

Risk due to V5: $15,165,000*(6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) + $40,000*(6%+6%+10%+30%+10%) +$6,000*(6%+6%+10%+30%+10%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(6%+6%+10%+30%+10%) + $50,000*(6%+6%+10%+30%+10%) + $3,033,000*(6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) = $7,882,984

Ranking of security asset residual risks: Ranking of security asset residual risks:

Rank	Asset	Value
1	A1: Financial Resources	$15,165,000
2	A4: Personnel Information	$9,199,089
3	A3: DMZ	$50,000
4	A22: LAN Server	$40,000
5	A25: Console	$40,000
6	A26: Router	$16,000
7	A24: VPN Server	$6000

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V3.4: Accidental Corruption and Loss of Data
2	V1.2: Unauthorized Access
3	V1.4: Unauthorized Modification of time and Attendance sheets
4	V4: Vulnerabilities Related to Disclosure or Brokerage of information
5	V5: Vulnerabilities Related to Network-Related Attacks

XIII. Conclusion:

Did the HGA team address all security risks based on your risk assessment for HGA?

No, HGA did not address all the security risks based on risk assessment. However, most of the crucial security risks have been addressed.

What would the budget for proposed controls be including controls proposed by new CISO controls and missing MOT controls and VPN and DMZ?

Controls	Estimated Budget
Controls Mitigating Vulnerabilities Related to Payroll Fraud	$100,000
Controls Mitigating Payroll Error	$75,000
Controls Mitigating Vulnerabilities Related to Continuity of Operations	$500,000
Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of information	$250,000
Controls Vulnerabilities Related to Network-Related Attacks	$200,000
Review of Security Controls	$50,000
Personnel Security	$300,000
VPN	$6000
DMZ	$50,000
Total	$1,531,000

Do you recommend a Risk Prevention Strategy or a Risk Response Strategy or a combination of both?

HGA has information systems which consists of sensitive information like financial resources, personnel information and intangible assets like reputation and employee confidence. Hence, it a Risk-Averse organization. Being a Risk-Averse organization, I recommend that the company employs a Risk prevention strategy.

Does the residual risk reduction exceed the budget for proposed controls?

Residual Risk Reduction = Residual risk with current controls – Residual risk with current controls, new controls, missing MOT controls, VPN and DMZ (mixed strategy)

= $30,056,000 - $12,384,089

= $17,671,911

Thus, residual risk reduction exceeds the budget for proposed controls.

What is the ((proposed security risk budget Cost) / (expected security risk Benefit)) ratio?

Cost Benefit ratio = (proposed security risk budget cost) / (expected security risk benefit)

= $1,531,000 / $17,671,911

= 0.0866

Part B: Security Risk Management Implementation Plan (based on Assignments 6-11)

List company critical assets, missing controls, vulnerabilities, potential threats, and security risks for:

Company Critical Assets

- Data is the most important asset at our company.

- Patients health records: Maintaining Patients health records is crucial to our organization. It will cost millions if there is any breach involving patient's health records.

- Client Information: Doctors and patient's information are one of the crucial assets. Damage control will cost millions if there are any data leaks.

- Employee Information: It consists of HR records. Damage control and credit monitoring services would cost the company millions of dollars of there is a breach.

- Organization Reputation: Positive Reputation for a corporation is essential for building trust and is one of the critical assets. It is intangible.

- Network Devices and software: There are numerous network devices and software which could be categorized as critical assets. As Data is the most important asset, servers like SQL database are the most critical assets at our organization. Other important assets include Servers, firewalls, routers, Cisco IPS etc. These network devices and applications cost hundreds of thousands of dollars.

S. No	Asset	Value (Approx.)
1	Patient Health Records	$200 Million
2	Client Information	$100 Million
3	Employee Information	$10 Million
4	Organization Reputation	Intangible
5	Network Devices	$5 Million

1. Access Control Security Risk Management Implementation Controls and Policies

S. No	IA Controls	Missing Control
a	Identification Credentials	- Biometric reference samples
b	Personal Authentication	- Biometric reference Sample - Privilege token database
c	Authorization	-
d	Logical Access Control methods	- Physical Security for Secure Internet Protocol Router Network (SIPRNet) Ports - Logical Network Port Security - Alternative login token
e	Physical Access Control Methods	- Defense Biometric Identification System (DBIDS)
f	Biometric Systems	- Fingerprint Scanner - Face Detection

Vulnerabilities

- As biometric reference samples are not implemented it can lead to poor identification and authentication.
- Secure Internet Protocol Router Network (SIPRNeT) Port are not implemented at my company.
- As logical port security is not implemented, ports are vulnerable to all kind of attacks.
- Unauthorized modification
- Vulnerabilities related to network related attacks

Threats

- Network Related Attacks
- There can be an array of attacks on ports as logical port security is not implemented.
- Poor authentication can lead to malicious users entering the network and wreaking havoc.
- Loss of Reputation
- Disclosure of sensitive information

Risks

- Unauthorized access
- Loss of Authentication
- Disclosure of sensitive information
- Loss of integrity
- Denial of service due to vulnerable ports.

2. Network Infrastructure Security Risk Management Implementation Controls and Policies

S. No	IA Controls	Missing Control
a	Enclave Protection	- Network Test Access Ports - Wireless IDS - Backdoor Connections
b	Firewalls Risk Management	- Deep Packet Inspection - Hybrid Technology Firewalls
c	Routers Risk Management	- Finger Service

- **Vulnerabilities**

  - My organization uses Port Mirroring (SPAN) instead Network Test Access Ports for packet capture. Quality data is not available for monitoring.
  - In my organization, Wireless IDS (WIDS) is not implemented. WIDS helps in detection of wireless DOS attacks.
  - Deep packet inspection and hybrid technology firewalls are missing in my organization which play a key role in detection of trojans email viruses etc.
  - Finger Services is not disabled in my organization which provides presence information which can be really useful for hackers.
  - Backdoor connections are missing in my organization. Admins cannot get into systems if an attacker compromises and takes control.

- **Threats**

  - Span ports are used instead of network TAPs (Test Access Points), which result in data quality issues like dropping of packets, alteration of packets etc. This information may be crucial for an organization as they depend on this to detect all types of attacks or intrusions.
  - WLAN attacks cannot be detected due to the absence of WIDS as they are different from their wired counterparts. Also, knowing details of DOS attacks, like where the attack is originating from and when they would occur; would be difficult without WIDS.
  - Due to the absence of Deep packet inspection and hybrid technology firewalls only header part evaluation would be possible. Inspection of data part is also crucial as we can weed out any non-compliant protocols, intrusions and spam, which isn't possible here.

- As Finger Service is not disabled, the user login information can be collected and be used for social engineering scams.
- Attackers can wreak havoc as the staff fail to get control back from the attackers due to missing backdoor connections.

- **Risks**

- Unauthorized access: Due to the absence of network TAPs, data cannot be properly monitored and collected. This can lead to unauthorized access not being detected.
- Disclosure of sensitive information: As Deep packet inspection and hybrid firewalls are not implemented, content leaving the organization cannot be detected. Data being one of the most crucial assets, disclosure of confidential information is one of the serious risks to our organization.
- Loss of confidentiality is a possibility as finger service is not disabled.
- Denial of Service: DOS attacks are also a possibility due to the few missing controls. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals is paramount.
- There can be a potential loss of availability as attacks can take control and there are no backdoor connections to get them back.

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

S. No	IA Controls	Missing Control
a	Ports, Protocols and Services	- IPv6 Address Filtering
b	Device Management	- Out of band Management
c	Device Monitoring	- SNMP Management
d	Network Authentication, Authorization and Auditing (AAA)	-
e	Network Intrusion Detection Systems (NIDS)	- Signature based, Anomaly based or rule-based NIDS
f	Switches, VLANS	- Intermediate Distribution Frames - Usage of sticky addresses in VLAN
g	VPN	- Host-to-Host

- **Vulnerabilities**

  - Out of Band Management is not implemented in my organization. This is a powerful tool for the management of critical devices which serve as a backbone for the company – for e.g. OOBM allows to remotely manage the devices even if the network is down or OS has crashed.
  - In Band Management is used in my company which has many inherent vulnerabilities. Although SSH with 1024-bit RSA keys are used, the key size is small compared to today's standards.
  - Both SNMP versions 2 and 3 are implemented at my company. Although SNMPv3 is secure, SNMPv2 still uses deprecated standards like MD5 and DES.
  - Signature-based, Anomaly-based or rule-based NIDS is not implemented and as a result the threat detection and analysis could not be performed effectively at the enclave gateways.
  - Due to the absence of Host-to-Host VPN a secured data transfer cannot be guaranteed.

- **Threats**

    - As Out of Band Management is not implemented, power outages and unplanned downtime can be possible threats which could result in a possible Denial of service.
    - Eavesdropping and other attacks would be possible due to the low-bit RSA key size used for In band management.
    - DOS attacks, scanning attacks and other malware could hit the network in the absence of an external NIDS which usually serve as first line of defense.
    - In the absence of host-to-host VPN attacks on database or servers could be possible as there is no reliable way of communication.

- **Risks**

    - Denial of Service: DOS attacks are also a possibility due to the absence of OOBM and external NIDS. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount.
    - Unauthorized access: Due to the absence of external NIDS, external network traffic cannot be monitored properly and malicious activities like unauthorized access may not be detected.
    - Disclosure of sensitive information: Attacks like eavesdropping can play a role in disclosure of information
    - Data confidentiality, Integrity and Authenticity can be compromised due to the absence of Host-to-Host VPN.

4. Database Security Risk Management Implementation Controls and Policies

S. No	IA Controls	Missing Control
a	Authentication – User Accounts	- Application User Manager
b	Authorization	- Multi-tier applications
c	Confidentiality	-
d	Data Integrity	-
e	Auditing	-
f	Replication and Federation	- Federated Databases
g	Clustering	- Database Clustering - Accountability - Protect Communication Path
h	Backup and Recovery	-
i	Operating System Protection	-
j	Application Protection	-
k	Network Protection	- Time and Count limits on Network Session Parameters
l	Security Design and Configuration	- Functional Architecture for IS Applications - Configuration Management (CM) Process - System Library Management Controls - Security Support Structure Portioning - Software Baseline
m	Enclave and Computing Environment	- Access for Need-to-know - Interconnection among DoD systems and Enclaves - Logon - Production Code Change Control - Resource Control - Security Configuration Compliance - Software Development Change Controls - Warning Message - Boundary Defense - Remote Access for Privileged Functions
n	Business Continuity	- Trusted Recovery
o	Vulnerability and Incident Management	-

- **Vulnerabilities**
    - The Time and Count limits on Network session parameters is not implemented in my organization. The most common time limit set for sessions in 10 min although Web Admins usually set it for 8 min.
    - Federated databases and database Clustering are not implemented at my company. They improve data distribution across multiple databases.
    - As configuration management practices are not followed it would be difficult to recover from malicious attacks. It also leads to more efficient change management.
    - Due to missing Security Support Structure Positioning, it is easy for malicious users to access the security policies.
    - Boundary defense is not implemented in my company and thus be vulnerability to many network related attacks.

- **Threats**
    - In the event of a DOS attack, the recovery might be difficult due to the missing of clustering and federation features like load balancing, high availability support thereby increasing downtime costing the company thousands of dollars.
    - In the absence of security support structure positioning, malicious user may change the security policies which may result in a whole range of compliance issues.
    - As Time and Count limits on Network session parameters is not implemented, several malicious attacks like session hijacking could be possible.
    - DOS attacks and malware can spread on the internal network as boundary defenses are not implemented.

- **Risks**
    - Denial of Service: DOS attacks are a possibility due to the absence of boundary defenses and recovery can be difficult due to missing controls like clustering and federation. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount.
    - Unauthorized access: Due to the absence of security support structure positioning, and boundary defenses, malware can spread through the internal network and unauthorized access is a possibility.
    - Disclosure of sensitive information: Attacks like Session hijacking can lead to stealing and disclosure of sensitive information.
    - Data confidentiality, Integrity and Authenticity can be compromised as general users can access the security policies of an organization.

5. Applications Development Security Risk Management Implementation Controls and Policies

S. No	IA Controls	Missing Control
a	Application Data Handling	- In-Memory Data Handling - Data Marking
b	Authentication	- Combination Client Server Application Authentication - PKI Certificate Validation
c	Cryptography	- Message Authentication codes, Hashes
d	User Accounts	- Application Sessions - Excessive Privileges
e	Input Validation	-
f	Auditing	- Classified audit record content
g	Configuration Management	-
h	Testing	- Automated Tools - Third party and open source catalog
i	Deployment	-

- **Vulnerabilities**

  - In my company the data in memory is not cleared after its use. This may lead to range of vulnerabilities including data being read or altered by malicious users.
  - Data Marking policies are not implemented at my company. This can lead to leak of sensitive information and IP data
  - As strict PKI validation policies are not followed, this can undermine the effectiveness of PKI certificates.
  - Hashes are not used in my company, instead encrypted passwords are stored. This can be a vulnerability if the attacker manages to gain access to keys which are not cleared from memory.
  - Session limits like time limits, limits on users and sessions in use are not implemented in my company.

- **Threats**

  - Denial of service and other attacks are possible through multiple logons as there are no session limits implemented.
  - As data in memory is not managed properly, a range of attacks would be possible from prediction of patterns to reconstruction of RSA and AES keys.
  - Several broken authentication attacks are possible as Message authentication codes and hashes are not implemented.

- As PKI validation policies are not implemented properly, denial of service and many attacks against PKI are possible.
- As DoD policies are followed only when dealing with government projects, during general use the code may be replaced by a malicious code.

- **Risks**

- Denial of Service: DOS attacks are a possibility due to absence of application sessions and PKI validation policies. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount.
- Unauthorized access: Due to the poor in-memory data handling policies, unauthorized access is a possibility after the attacker learns about the cryptographic keys from the memory.
- Disclosure of sensitive information: Absence of data marking can lead to disclosure of sensitive information and IP data.
- Data Integrity and Authenticity can be compromised as message authentication codes and hashes are not used.
- Data confidentiality can be compromised as data in memory can be accessed by a malicious user.

6. Wireless Security Risk Management Implementation Controls and Policies

S. No	IA Controls	Missing Control
a	Wireless LAN Risk Management	- Extensible Authentication protocol (EAP) - EAP Tunneling Transport Layer Security (EAP-TTLS) - Protected EAP (PEAP) - Lightweight EAP (LEAP) - EAP-MD5 - Authorized Architecture - Wired Equivalent Privacy (WEP) - Wi-Fi Protected Access (WPA) - RSN - Windows 2000 and XP systems
b	Wireless PAN Risk Management	- PIN/Legacy Pairing
c	Wireless WAN Risk Management	- Wireless WAN security Protocols - 802.16 Broadband Wireless Access (BWA) Standard - Mobile WiMAX
d	Wireless RFID Risk Management	- Types of RFID Systems - RFID Attack Methods
e	Wireless PED Risk Management	- Wireless Two-Way Email - Secure Mobile Environment PED (SME PED)

- **Vulnerabilities**

  - Protected EAP is not implemented at my company. This method of tunneling the network communication can provide additional security.
  - My organization does not implement authorized architecture. This missing wireless risk management policy can lead to poor security of access points and bridges. Rogue access points and Evil twin access points can be easily be created.
  - Robust security network (RSN) is not implemented at my company. This can lead to poor authentication, encryption and key management services.
  - Secure Wireless networking and security boundary controls are Implemented only when dealing with government projects. This can be a vulnerability during non-government projects.
  - Wireless two-way email is not implemented at my organization. This can be a potential vulnerability.

- **Threats**

    - Denial of service, broken authentication attacks and MAC address spoofing are possible due to the absence of RSN.
    - As authorized architecture is not implemented this can lead to DOS and sniffing attacks with a simple application like ethereal.
    - As Secure Wireless networking and security boundary controls are not Implemented, several network related threats are possible from phishing attacks to Advanced Persistent Threats.
    - Email messages can be obtained by malicious users as secure wireless two-way email is not used.
    - SSIDs are not hidden at my company. This can make attackers work easy for launching a successful attack.

- **Risks**

    - Denial of Service: DOS attacks are a possibility due to absence of RSN and authorized architecture. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount.
    - Unauthorized access: Due to the absence of RSN and authorized architecture, MAC address spoofing and sniffing attacks are possible which can lead to unauthorized access.
    - Disclosure of sensitive information: As Secure Wireless networking and security boundary controls are not implemented for non-government projects, disclosure of sensitive data can be a possibility.
    - Data integrity and confidentiality can be compromised as wireless two-way email is not used.
    - Data confidentiality can be compromised as secure tunneling method like PEAP in not used for network communication.

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

IA Controls	Implementation Control
Identification Credentials	- ID Card - Photograph - Password - Digital Signatures - PIN's - PKI Certificate
Personal Authentication	- Password - Smart Card - Access control lists - Policies
Authorization	- Access control lists - Security tokens - Deny by default policy
Logical Access Control methods	- Network Architecture controls - Remote Network Access - Security Network ports - Port Authentication using 802.1x - Network Access Control systems - Passwords - PIN's - Encryption - PKI Compliance Requirements - DoD Common Access Card
Physical Access Control Methods	- Badges - Smart cards - Physical Tokens - Physical Intrusion Detection Systems
Biometric Systems	-
Enclave Protection	- Defense in Depth - Firewalls - Routers - IDS/IPS - Encryption - Enclave DMZ - IPSec VPN Tunnel
Firewalls Risk Management	- Packet Filters - Bastion Host - Stateful Inspection - Application Proxy Gateway - Proxy Servers - DMZ and Content Filtering
Routers Risk Management	- Static Routers

	- Neighbor Router Authentication - Authenticate Routing Protocol - Packet Assembler Dissembler - Logging Integrity - Router Control Policy
Ports, Protocols and Services	- Block ICMPv4 Echo request and reply Packets - Disable Traceroute - Restrict Inbound and Outbound traffic - Unicast Reverse Path Forwarding - SYN Flood Attacks
Device Management	- Vulnerability Management System - Current Version of Software and firmware - WAN Implementation - In band Implementation - SSH Implementation
Device Monitoring	- SNMP - Network Management Station
Network Authentication, Authorization and Auditing (AAA)	- Network Authentication - Network Authorization - Network Auditing - Implementation of Authentication Server - Two Factor Authentication - Implementation of Syslog Server - Router Password Protection
Network Intrusion Detection Systems (NIDS)	- Enclave NIDS
Switches, VLANS	- VLANs - Separation of Users - VLAN Trunking - VLAN Port Security - VLAN Management Policy Server
VPN	- Gateway-to-Gateway - Host-to-Gateway
Authentication – User Accounts	- DBMS - Application User - DBA - Application Owner - Application Account - Database Auditor - Database Operator - Passwords - Certificates - External Authentication - Credential Storage
Authorization	- RBAC - Rename default accounts
Confidentiality	- Data Encryption

	- Application Code - Encrypt Data Files - Database Configuration, Transaction logs and Audit trails
Data Integrity	- Transaction Logs - Database Integrity
Auditing	- Audit logs Protections - Audit logs Retention - Audit Reporting
Replication and Federation	- Database Links - Database Replication
Clustering	-
Backup and Recovery	- DBMS Backup - Database Recovery
Operating System Protection	- Database Directories and Files - Dedicated OS Account - Database Software
Application Protection	- Input validation - Review Authentication Method - Minimum Privileges
Network Protection	- Network Access Protection - Protection against Unauthorized Disclosure
Security Design and Configuration	- Procedural Review - Configuration and Specification - Compliance Testing - Non-Repudiation - Partitioning and application - Ports, Protocols and Services - IA Documentation - Group Identification and Authentication - Individual Identification and Authentication - Key Management - Token and Certificate Standards
Enclave and Computing Environment	- Audit Record Content - Audit trail, Monitoring, Analysis and Reporting - Changes to Data - Encryption for Confidentiality: Data at Rest - Encryption for Confidentiality: Data in Transit - Data Change Controls - Audit of Security Label Changes - Audit Reduction and Report Generation - Audit Record Retention - Audit Trail Backup - Audit Trail Protection - Account Control
Business Continuity	- Protection of Backup and Restoration Assets - Data Backup Procedures - Disaster and Recovery Planning

	- Backup Copies of Critical Software
Vulnerability and Incident Management	- Vulnerability Management
Application Data Handling	- Database Management System - Data Storage - Data Transmission - Data Integrity
Authentication	- Server Authentication - User Authentication - Signed Code Identification - Standalone Application Authentication - Server Application Authentication - Client Application Authentication - Application Component Authentication - Password Complexity and Maintenance - Credential Protection
Cryptography	- Symmetric Ciphers - Digital Signatures
User Accounts	- Application Accounts - Access Controls
Input Validation	- Integer Overflows - Format String vulnerability - Command Injection Vulnerability - Buffer Overflows - Canonical Representation - Hidden Field Vulnerability - Information Disclosure - Race condition
Auditing	- Notify the User on login - Access to need-to-know information - Mobile code - Web Services
Configuration Management	- Software CM - Release Manager
Testing	- Plans and Procedures - Fuzzy testing - Code Reviews - Web Application Vulnerability Scanners
Deployment	- Documentation - Maintenance - Denial of Service - Audit Trail Monitoring - Audit Log Retention - Audit Trail Protection - Recovery and Contingency Planning - Account Management - Deployment Infrastructure

Wireless LAN Risk Management	- IEEE 802.11 WLAN System Standard - EAP Transport Layer security (EAP-TLS) - Wireless Station/Client - Wireless Network Interface Cards - Access Point - WPA2 - IP Security (IPSec) - WLAN Security - Service Set Identifier (SSID) - MAC Address - Secure Wireless networking (DoD Requirements) - Security Boundary Implementations (DoD)
Wireless PAN Risk Management	- Frequency-Hopping Spread Spectrum - Device Versions - Power Management - Security Modes and Levels - Secure Simple Pairing - Security standards - Mice and Keyboards
Wireless WAN Risk Management	-
Wireless RFID Risk Management	-
Wireless PED Risk Management	- Cellular Technologies - Short Messaging Service (SMS) - Multimedia Messaging Service (MMS) - PDA Security

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

IA Controls	Implementation Control	Status
Identification Credentials	- ID Card - Photograph - Password - Digital Signatures - PIN's - PKI Certificate	Present
	- Biometric reference samples	Absent
Personal Authentication	- Password - Smart Card - Access control lists - Policies	Present
	-	Absent

Authorization	- Access control lists - Security tokens - Deny by default policy	Present
	- Biometric reference Sample - Privilege token database	Absent
Logical Access Control methods	- Network Architecture controls - Remote Network Access - Security Network ports - Port Authentication using 802.1x - Network Access Control systems - Passwords - PIN's - Encryption - PKI Compliance Requirements - DoD Common Access Card	Present
	- Physical Security for Secure Internet Protocol Router Network (SIPRNet) Ports - Logical Network Port Security - Alternative login token	Absent
Physical Access Control Methods	- Badges - Smart cards - Physical Tokens - Physical Intrusion Detection Systems	Present
	- Defense Biometric Identification System (DBIDS)	Absent
Biometric Systems	-	Present
	- Fingerprint Scanner - Face Detection	Absent
Enclave Protection	- Defense in Depth - Firewalls - Routers - IDS/IPS - Encryption - Enclave DMZ - IPSec VPN Tunnel	Present
	- Network Test Access Ports - Wireless IDS - Backdoor Connections	Absent
Firewalls Risk Management	- Packet Filters - Bastion Host - Stateful Inspection - Application Proxy Gateway - Proxy Servers - DMZ and Content Filtering	Present
	- Deep Packet Inspection - Hybrid Technology Firewalls	Absent

Routers Risk Management	- Static Routers - Neighbor Router Authentication - Authenticate Routing Protocol - Packet Assembler Dissembler - Logging Integrity - Router Control Policy	Present
	- Finger Service	Absent
Ports, Protocols and Services	- Block ICMPv4 Echo request and reply Packets - Disable Traceroute - Restrict Inbound and Outbound traffic - Unicast Reverse Path Forwarding - SYN Flood Attacks	Present
	- IPv6 Address Filtering	Absent
Device Management	- Vulnerability Management System - Current Version of Software and firmware - WAN Implementation - In band Implementation - SSH Implementation	Present
	- Out of band Management	Absent
Device Monitoring	- SNMP - Network Management Station	Present
	- SNMP Management	Absent
Network Authentication, Authorization and Auditing (AAA)	- Network Authentication - Network Authorization - Network Auditing - Implementation of Authentication Server - Two Factor Authentication - Implementation of Syslog Server - Router Password Protection	Present
	-	Absent
Network Intrusion Detection Systems (NIDS)	- Enclave NIDS	Present
	- Signature based, Anomaly based or rule-based NIDS	Absent
Switches, VLANS	- VLANs - Separation of Users - VLAN Trunking - VLAN Port Security - VLAN Management Policy Server	Present
	- Intermediate Distribution Frames - Usage of sticky addresses in VLAN	Absent
VPN	- Gateway-to-Gateway - Host-to-Gateway	Present
	- Host-to-Host	Absent

Authentication – User Accounts	- DBMS - Application User - DBA - Application Owner - Application Account - Database Auditor - Database Operator - Passwords - Certificates - External Authentication - Credential Storage	Present
	- Application User Manager	Absent
Authorization	- RBAC - Rename default accounts	Present
	- Multi-tier applications	Absent
Confidentiality	- Data Encryption - Application Code - Encrypt Data Files - Database Configuration, Transaction logs and Audit trails	Present
	-	Absent
Data Integrity	- Transaction Logs - Database Integrity	Present
	-	
Auditing	- Audit logs Protections - Audit logs Retention - Audit Reporting	Present
	-	Absent
Replication and Federation	- Database Links - Database Replication	Present
	- Federated Databases	Absent
Clustering	-	Present
	- Database Clustering - Accountability - Protect Communication Path	Absent
Backup and Recovery	- DBMS Backup - Database Recovery	Present
	-	Absent
Operating System Protection	- Database Directories and Files - Dedicated OS Account - Database Software	Present
	-	Absent
Application Protection	- Input validation - Review Authentication Method - Minimum Privileges	Present
	-	Absent

Network Protection	- Network Access Protection - Protection against Unauthorized Disclosure	Present
	- Time and Count limits on Network Session Parameters	Absent
Security Design and Configuration	- Procedural Review - Configuration and Specification - Compliance Testing - Non-Repudiation - Partitioning and application - Ports, Protocols and Services - IA Documentation - Group Identification and Authentication - Individual Identification and Authentication - Key Management - Token and Certificate Standards	Present
	- Functional Architecture for IS Applications - Configuration Management (CM) Process - System Library Management Controls - Security Support Structure Portioning - Software Baseline	Absent
Enclave and Computing Environment	- Audit Record Content - Audit trail, Monitoring, Analysis and Reporting - Changes to Data - Encryption for Confidentiality: Data at Rest - Encryption for Confidentiality: Data in Transit - Data Change Controls - Audit of Security Label Changes - Audit Reduction and Report Generation - Audit Record Retention - Audit Trail Backup - Audit Trail Protection - Account Control	Present
	- Access for Need-to-know - Interconnection among DoD systems and Enclaves - Logon - Production Code Change Control - Resource Control - Security Configuration Compliance - Software Development Change Controls - Warning Message - Boundary Defense - Remote Access for Privileged Functions	Absent
Business Continuity	- Protection of Backup and Restoration Assets - Data Backup Procedures - Disaster and Recovery Planning - Backup Copies of Critical Software	Present
	- Trusted Recovery	Absent

Vulnerability and Incident Management	- Vulnerability Management	Present
	-	Absent
Application Data Handling	- Database Management System - Data Storage - Data Transmission - Data Integrity	Present
	- In-Memory Data Handling - Data Marking	Absent
Authentication	- Server Authentication - User Authentication - Signed Code Identification - Standalone Application Authentication - Server Application Authentication - Client Application Authentication - Application Component Authentication - Password Complexity and Maintenance - Credential Protection	Present
	- Combination Client Server Application Authentication - PKI Certificate Validation	Absent
Cryptography	- Symmetric Ciphers - Digital Signatures	Present
	- Message Authentication codes, Hashes	Absent
User Accounts	- Application Accounts - Access Controls	Present
	- Application Sessions - Excessive Privileges	Absent
Input Validation	- Integer Overflows - Format String vulnerability - Command Injection Vulnerability - Buffer Overflows - Canonical Representation - Hidden Field Vulnerability - Information Disclosure - Race condition	Present
	-	Absent
Auditing	- Notify the User on login - Access to need-to-know information - Mobile code - Web Services	Present
	- Classified audit record content	Absent
Configuration Management	- Software CM - Release Manager	Present
	-	Absent

Testing	- Plans and Procedures - Fuzzy testing - Code Reviews - Web Application Vulnerability Scanners	Present
	- Automated Tools - Third party and open source catalog	Absent
Deployment	- Documentation - Maintenance - Denial of Service - Audit Trail Monitoring - Audit Log Retention - Audit Trail Protection - Recovery and Contingency Planning - Account Management - Deployment Infrastructure	Present
	-	Absent
Wireless LAN Risk Management	- IEEE 802.11 WLAN System Standard - EAP Transport Layer security (EAP-TLS) - Wireless Station/Client - Wireless Network Interface Cards - Access Point - WPA2 - IP Security (IPSec) - WLAN Security - Service Set Identifier (SSID) - MAC Address - Secure Wireless networking (DoD Requirements) - Security Boundary Implementations (DoD)	Present
	- Extensible Authentication protocol (EAP) - EAP Tunneling Transport Layer Security (EAP-TTLS) - Protected EAP (PEAP) - Lightweight EAP (LEAP) - EAP-MD5 - Authorized Architecture - Wired Equivalent Privacy (WEP) - Wi-Fi Protected Access (WPA) - RSN - Windows 2000 and XP systems	Absent
Wireless PAN Risk Management	- Frequency-Hopping Spread Spectrum - Device Versions - Power Management - Security Modes and Levels - Secure Simple Pairing - Security standards - Mice and Keyboards	Present
	- PIN/Legacy Pairing	Absent
	-	Present

Wireless WAN Risk Management	- Wireless WAN security Protocols - 802.16 Broadband Wireless Access (BWA) Standard - Mobile WiMAX	Absent
Wireless RFID Risk Management	-	Present
	- Types of RFID Systems - RFID Attack Methods	Absent
Wireless PED Risk Management	- Cellular Technologies - Short Messaging Service (SMS) - Multimedia Messaging Service (MMS) - PDA Security	Present
	- Wireless Two-Way Email - Secure Mobile Environment PED (SME PED)	Absent

c. List of critical assets that exist in your company

Company Critical Assets

- Data is the most important asset at our company.

- Patients health records: Maintaining Patients health records is crucial to our organization. It will cost millions if there is any breach involving patient's health records.

- Client Information: Doctors and patient's information are one of the crucial assets. Damage control will cost millions if there are any data leaks.

- Employee Information: It consists of HR records. Damage control and credit monitoring services would cost the company millions of dollars of there is a breach.

- Organization Reputation: Positive Reputation for a corporation is essential for building trust and is one of the critical assets. It is intangible.

- Network Devices and software: There are numerous network devices and software which could be categorized as critical assets. As Data is the most important asset, servers like SQL database are the most critical assets at our organization. Other important assets include Servers, firewalls, routers, Cisco IPS etc. These network devices and applications cost hundreds of thousands of dollars.

S. No	Asset	Value (Approx.)
1	Patient Health Records	$200 Million
2	Client Information	$100 Million
3	Employee Information	$10 Million
4	Organization Reputation	Intangible
5	Network Devices	$5 Million

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

- As biometric reference samples are not implemented it can lead to poor identification and authentication.
- Secure Internet Protocol Router Network (SIPRNeT) Port are not implemented at my company.
- As logical port security is not implemented, ports are vulnerable to all kind of attacks.
- Unauthorized modification
- Vulnerabilities related to network related attacks
- My organization uses Port Mirroring (SPAN) instead Network Test Access Ports for packet capture. Quality data is not available for monitoring.
- In my organization, Wireless IDS (WIDS) is not implemented. WIDS helps in detection of wireless DOS attacks.
- Deep packet inspection and hybrid technology firewalls are missing in my organization which play a key role in detection of trojans email viruses etc.
- Finger Services is not disabled in my organization which provides presence information which can be really useful for hackers.
- Out of Band Management is not implemented in my organization. This is a powerful tool for the management of critical devices which serve as a backbone for the company – for e.g. OOBM allows to remotely manage the devices even if the network is down or OS has crashed.
- In Band Management is used in my company which has many inherent vulnerabilities. Although SSH with 1024-bit RSA keys are used, the key size is small compared to today's standards.
- Both SNMP versions 2 and 3 are implemented at my company. Although SNMPv3 is secure, SNMPv2 still uses deprecated standards like MD5 and DES.
- Signature-based, Anomaly-based or rule-based NIDS is not implemented and as a result the threat detection and analysis could not be performed effectively at the enclave gateways.
- Due to the absence of Host-to-Host VPN a secured data transfer cannot be guaranteed.
- The Time and Count limits on Network session parameters is not implemented in my organization. The most common time limit set for sessions in 10 min although Web Admins usually set it for 8 min.

- Federated databases and database Clustering are not implemented at my company. They improve data distribution across multiple databases.
- As configuration management practices are not followed it would be difficult to recover from malicious attacks. It also leads to more efficient change management.
- Due to missing Security Support Structure Positioning, it is easy for malicious users to access the security policies.
- Boundary defense is not implemented in my company and thus be vulnerability to many network related attacks.
- In my company the data in memory is not cleared after its use. This may lead to range of vulnerabilities including data being read or altered by malicious users.
- Data Marking policies are not implemented at my company. This can lead to leak of sensitive information and IP data
- As strict PKI validation policies are not followed, this can undermine the effectiveness of PKI certificates.
- Hashes are not used in my company, instead encrypted passwords are stored. This can be a vulnerability if the attacker manages to gain access to keys which are not cleared from memory.
- Session limits like time limits, limits on users and sessions in use are not implemented in my company.
- Protected EAP is not implemented at my company. This method of tunneling the network communication can provide additional security.
- My organization does not implement authorized architecture. This missing wireless risk management policy can lead to poor security of access points and bridges. Rogue access points and Evil twin access points can be easily be created.
- Robust security network (RSN) is not implemented at my company. This can lead to poor authentication, encryption and key management services.
- Secure Wireless networking and security boundary controls are Implemented only when dealing with government projects. This can be a vulnerability during non-government projects.

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

- Network Related Attacks
- There can be an array of attacks on ports as logical port security is not implemented.
- Poor authentication can lead to malicious users entering the network and wreaking havoc.
- Loss of Reputation
- Disclosure of sensitive information

- Span ports are used instead of network TAPs (Test Access Points), which result in data quality issues like dropping of packets, alteration of packets etc. This information may be crucial for an organization as they depend on this to detect all types of attacks or intrusions.
- WLAN attacks cannot be detected due to the absence of WIDS as they are different from their wired counterparts. Also, knowing details of DOS attacks, like where the attack is originating from and when they would occur; would be difficult without WIDS.
- Due to the absence of Deep packet inspection and hybrid technology firewalls only header part evaluation would be possible. Inspection of data part is also crucial as we can weed out any non-compliant protocols, intrusions and spam, which isn't possible here.
- As Finger Service is not disabled, the user login information can be collected and be used for social engineering scams.
- As Out of Band Management is not implemented, power outages and unplanned downtime can be possible threats which could result in a possible Denial of service.
- Eavesdropping and other attacks would be possible due to the low-bit RSA key size used for In band management.
- DOS attacks, scanning attacks and other malware could hit the network in the absence of an external NIDS which usually serve as first line of defense.
- In the absence of host-to-host VPN attacks on database or servers could be possible as there is no reliable way of communication.
- In the event of a DOS attack, the recovery might be difficult due to the missing of clustering and federation features like load balancing, high availability support thereby increasing downtime costing the company thousands of dollars.
- In the absence of security support structure positioning, malicious user may change the security policies which may result in a whole range of compliance issues.
- As Time and Count limits on Network session parameters is not implemented, several malicious attacks like session hijacking could be possible.
- DOS attacks and malware can spread on the internal network as boundary defenses are not implemented.
- Denial of service and other attacks are possible through multiple logons as there are no session limits implemented.
- As data in memory is not managed properly, a range of attacks would be possible from prediction of patterns to reconstruction of RSA and AES keys.
- Several broken authentication attacks are possible as Message authentication codes and hashes are not implemented.
- As PKI validation policies are not implemented properly, denial of service and many attacks against PKI are possible.
- As DoD policies are followed only when dealing with government projects, during general use the code may be replaced by a malicious code.

- Denial of service, broken authentication attacks and MAC address spoofing are possible due to the absence of RSN.
- As authorized architecture is not implemented this can lead to DOS and sniffing attacks with a simple application like ethereal.
- As Secure Wireless networking and security boundary controls are not Implemented, several network related threats are possible from phishing attacks to Advanced Persistent Threats.
- SSIDs are not hidden at my company. This can make attackers work easy for launching a successful attack.

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

- Unauthorized access
- Disclosure of sensitive information
- Loss of integrity
- Denial of service due to vulnerable ports.
- Loss of Authentication
- Unauthorized access: Due to the absence of network TAPs, data cannot be properly monitored and collected. This can lead to unauthorized access not being detected.
- Disclosure of sensitive information: As Deep packet inspection and hybrid firewalls are not implemented, content leaving the organization cannot be detected. Data being one of the most crucial assets, disclosure of confidential information is one of the serious risks to our organization.
- Denial of Service: DOS attacks are also a possibility due to the few missing controls. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals is paramount.
- Denial of Service: DOS attacks are also a possibility due to the absence of OOBM and external NIDS. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount.
- Unauthorized access: Due to the absence of external NIDS, external network traffic cannot be monitored properly and malicious activities like unauthorized access may not be detected.
- Disclosure of sensitive information: Attacks like eavesdropping can play a role in disclosure of information
- Data confidentiality, Integrity and Authenticity can be compromised due to the absence of Host-to-Host VPN.
- Denial of Service: DOS attacks are a possibility due to the absence of boundary defenses and recovery can be difficult due to missing controls like clustering and federation. This

can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount.

- Unauthorized access: Due to the absence of security support structure positioning, and boundary defenses, malware can spread through the internal network and unauthorized access is a possibility.
- Disclosure of sensitive information: Attacks like Session hijacking can lead to stealing and disclosure of sensitive information.
- Data confidentiality, Integrity and Authenticity can be compromised as general users can access the security policies of an organization.
- Denial of Service: DOS attacks are a possibility due to absence of application sessions and PKI validation policies. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount.
- Unauthorized access: Due to the poor in-memory data handling policies, unauthorized access is a possibility after the attacker learns about the cryptographic keys from the memory.
- Disclosure of sensitive information: Absence of data marking can lead to disclosure of sensitive information and IP data.
- Data Integrity and Authenticity can be compromised as message authentication codes and hashes are not used.
- Data confidentiality can be compromised as data in memory can be accessed by a malicious user.
- Denial of Service: DOS attacks are a possibility due to absence of RSN and authorized architecture. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount.
- Unauthorized access: Due to the absence of RSN and authorized architecture, MAC address spoofing and sniffing attacks are possible which can lead to unauthorized access.
- Disclosure of sensitive information: As Secure Wireless networking and security boundary controls are not implemented for non-government projects, disclosure of sensitive data can be a possibility.
- Data confidentiality can be compromised as secure tunneling method like PEAP in not used for network communication.

g. List of recommended 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

i. Access Control Security Risk Management Implementation Controls and Policies

- Biometric systems need to be implemented for improved authentication. They provide improved security and also cannot be forgotten or lost.
- Implementing a deny by default policy on the company firewall provides us with a better control over authorization. All the ingress traffic from the internet is denied by default.
- Logical Network Port Security should be implemented so that all the unnecessary ports can be closed and be less susceptible to attacks from the internet.
- Data loss prevention software should be implemented to protect all the sensitive information and to tighten endpoint security

ii. Network Infrastructure Security Risk Management Implementation Controls and Policies

- Network TAPs needs to be implemented to monitor and detect malicious activities by analyzing quality packet captures.
- Wireless IDS need to be implemented to detect WLAN attacks and DOS attacks
- Implementation of deep packet inspection and hybrid firewall technologies is crucial as they can be able to detect malicious payload and prevent some critical cyber-attacks on the organization.

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

- Out of Band management should be implemented alongside In band management as it is one of the best practices to manage network devices effectively.
- Signature-based, Anomaly-based or rule-based NIDS needs to be implemented to efficiently detect DOS attacks and other malware.
- Host-to-Host VPN should be implemented for a secure IPSec connection using RSA between the hosts for secure data transfers and communications.

iv. Database Security Risk Management Implementation Controls and Policies

- Implementing Time and Count limits on Network session parameters can greatly increase the security of the database while prevent many malicious attack attempts.
- Boundary defense needs to be implemented which acts like a first line of defense to safeguard sensitive information and keep the malicious traffic out from the internal network.
- Warning messages can also be implemented to detect any malicious attempts.

- security support structure positioning should be implemented to ascertain the security policies are safeguarded from malicious users.

v. Applications Development Security Risk Management Implementation Controls and Policies

- All the data in memory should be cleared after use and all the data should also be encrypted in memory when not in use.
- Data marking policies should be implemented to avoid risk of information disclosure.
- PKI certificates validation should be enforced properly for the ascertain the effectiveness of PKI certificates.
- Message authentication codes and hashes should be implemented to ensure data confidentiality, integrity and availability.
- Session limits should be implemented to avoid DOS and other attacks.

vi. Wireless Security Risk Management Implementation Controls and Policies

- Additional protocols like PEAP should be used to ensure data confidentiality and integrity.
- Authorized architecture should be implemented to secure the wireless access points and bridges.
- Secure Wireless networking and security boundary controls must be implemented for all projects, not just govt. projects.
- RSN can be implemented to prevent MAC address spoofing and other sniffing attacks.

h. List of recommended Hardening methods and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience (it is not required to write detailed policies) – Risk Response Strategy

vii. Access Control Security Risk Management Implementation Controls and Policies

- Data Activity Monitoring (DAM) solution can be implemented to closely monitor traffic and to avoid data leaks. An average hacker conducts reconnaissance six months before the actual breach, hence monitoring for unusual behavior can help deter a data breach.
- A Host based Intrusion Detection System and Network based Intrusion Detection System can be implemented for closely monitoring, analyzing the packets, logging and notifying authorities.
- Full scans must be run for malware from time to time basis.

viii. Network Infrastructure Security Risk Management Implementation Controls and Policies

- Network TAPs and Data Activity Monitoring (DAM) solution can be implemented to closely monitor traffic and to avoid data leaks. An average hacker conducts reconnaissance six months before the actual breach, hence monitoring for unusual behavior can help deter a data breach.
- A Wireless Intrusion Detection System and Network based Intrusion Detection System can be implemented for closely monitoring, analyzing the packets, logging and notifying authorities.
- Full scans must be run for malware from time to time basis.
- Backdoors could be implemented by the organization for admins to regain control of the systems after the attacker has compromised and changed the credentials of the critical applications and services.

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

- It good to hire DDOS mitigation services which can handle high amounts of traffic and have data scrubbing centers in case of DOS attacks.
- RSA key sizes should be increased to 4096 bits to safeguard against any possible attacks
- SNMP Management system can be implemented to better analyze and monitor performance.
- SNMPv2 should be stopped and SNMPv3 should be adopted completely as it uses much secure AES encryption standard.

x. Database Security Risk Management Implementation Controls and Policies

- It is good to implement clustering and federated databases to recover quickly against DOS attacks and reduce downtime.
- Following good configuration management practices, the visibility, performance and efficiency can be increased deterring data breaches and reducing the risk of outages.
- security support structure positioning should be implemented to ascertain the security policies are safeguarded from malicious users
- In the event of system failures and corruptions trusted recovery can help recover thus promoting business continuity.

xi. Applications Development Security Risk Management Implementation Controls and Policies

- Security controls like ACL’s and permissions should be implemented for applications with excessive privileges.
- Automated tools should be implemented for testing which maximizes the chances of finding coding errors and other vulnerabilities.

- Combination of client server application authentication should be implemented to streamline the process of authentication.
- Classified Audit record content should be followed to classify and prioritize audit events.
- Use of open source catalog can be helpful in developing secure applications and testing policies should also be implemented by open source software.

xii. Wireless Security Risk Management Implementation Controls and Policies

- Wireless two-way email can be implemented for securing wireless emails for additional security.
- SSIDs can be made hidden which makes the attackers work harder to carry out a successful attack.
- Secure Mobile Environment PED can be used for secure voice and data communication.
- Bluetooth mice and keyboard should be replaced with wired counterparts.

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

a. HIPAA (Health Insurance Portability and Accountability Act)

My organization is related to healthcare industry and thus HIPAA is applicable. This law was enacted to improve the efficiency and effectiveness of healthcare systems. Some of the key controls for the protection of patients data privacy are Information access management, workforce security and regular security audits.

b. Federal Red Flag rules

The federal red flag rules are also applicable to healthcare industry and are used to combat identity theft. If any red flags are identified, they should be reported to the law enforcement.

c. Massachusetts security plan

This legislation applies to any company which stores, maintains personal information of residents of Massachusetts. Since my company maintains the PII information and medical records this regulation is applicable.

9. Rank asset risks and vulnerability risks for your company across Access Control, Network Infrastructure, Network Infrastructure Management, Database, Applications, and Wireless. For this step, you can create a table with columns or rows Access Control, Network Infrastructure, Network Infrastructure Management, Database, Applications, and Wireless, and in each cell place the top 5 or top 10 asset risks for each category. Then the same for vulnerability risks. Then you can discuss the top 5 asset risk across all categories and the top 5 vulnerability risks across all categories.

	Top 5 or 10 Asset risks	**Top 5 or 10 Vulnerability risks**
Access Controls	-As biometric reference samples are not implemented it can lead to poor identification and authentication. -Secure Internet Protocol Router --Network (SIPRNeT) Port are not implemented at my company. -As logical port security is not implemented, ports are vulnerable to all kind of attacks. -Unauthorized modification -Vulnerabilities related to network related attacks	-Disclosure of sensitive information -Loss of integrity -Unauthorized access -Denial of service due to vulnerable ports. -Loss of Authentication
Network Infrastructure	- Deep packet inspection and hybrid technology firewalls are missing in my organization which play a key role in detection of trojans email viruses etc. - Finger Services is not disabled in my organization which provides presence information which can be really useful for hackers. - My organization uses Port Mirroring (SPAN) instead Network Test Access Ports for packet capture. Quality data is not available for monitoring. - In my organization, Wireless IDS (WIDS) is not implemented. WIDS helps in detection of wireless DOS attacks. - Backdoor connections are missing in my organization.	- Unauthorized access: Due to the absence of network TAPs, data cannot be properly monitored and collected. This can lead to unauthorized access not being detected. - Disclosure of sensitive information: As Deep packet inspection and hybrid firewalls are not implemented, content leaving the organization cannot be detected. Data being one of the most crucial assets, disclosure of confidential information is one of the serious risks to our organization. - Denial of Service: DOS attacks are also a possibility due to the few missing controls. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals is paramount. - There can be a potential loss of availability as attacks can take

	Admins cannot get into systems if an attacker compromises and takes control.	control and there are no backdoor connections to get them back.
Network Infrastructure Management	- In Band Management is used in my company which has many inherent vulnerabilities. Although SSH with 1024-bit RSA keys are used, the key size is small compared to today's standards. - Both SNMP versions 2 and 3 are implemented at my company. Although SNMPv3 is secure, SNMPv2 still uses deprecated standards like MD5 and DES. - Signature-based, Anomaly-based or rule-based NIDS is not implemented and as a result the threat detection and analysis could not be performed effectively at the enclave gateways. - Due to the absence of Host-to-Host VPN a secured data transfer cannot be guaranteed. - Out of Band Management is not implemented in my organization. This is a powerful tool for the management of critical devices which serve as a backbone for the company – for e.g. OOBM allows to remotely manage the devices even if the network is down or OS has crashed.	- Unauthorized access: Due to the absence of external NIDS, external network traffic cannot be monitored properly and malicious activities like unauthorized access may not be detected. - Disclosure of sensitive information: Attacks like eavesdropping can play a role in disclosure of information. - Data confidentiality, Integrity and Authenticity can be compromised due to the absence of Host-to-Host VPN - Denial of Service: DOS attacks are also a possibility due to the absence of OOBM and external NIDS. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount
Database Security	- Federated databases and database Clustering are not implemented at my company. They improve data distribution across multiple databases. - As configuration management practices are not followed it would be difficult to recover from malicious attacks. It also leads to more efficient change management.	- Disclosure of sensitive information: Attacks like Session hijacking can lead to stealing and disclosure of sensitive information. - Data confidentiality, Integrity and Authenticity can be compromised as general users can access the security policies of an organization. - Denial of Service: DOS attacks are a possibility due to the absence of boundary defenses and recovery can be

	- The Time and Count limits on Network session parameters is not implemented in my organization. The most common time limit set for sessions in 10 min although Web Admins usually set it for 8 min. - Due to missing Security Support Structure Positioning, it is easy for malicious users to access the security policies. - Boundary defense is not implemented in my company and thus be vulnerability to many network related attacks	difficult due to missing controls like clustering and federation. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount. - Unauthorized access: Due to the absence of security support structure positioning, and boundary defenses, malware can spread through the internal network and unauthorized access is a possibility.
Application Security	- Data Marking policies are not implemented at my company. This can lead to leak of sensitive information and IP data - As strict PKI validation policies are not followed, this can undermine the effectiveness of PKI certificates. - In my company the data in memory is not cleared after its use. This may lead to range of vulnerabilities including data being read or altered by malicious users. - Hashes are not used in my company, instead encrypted passwords are stored. This can be a vulnerability if the attacker manages to gain access to keys which are not cleared from memory. - Session limits like time limits, limits on users and sessions in use are not implemented in my company.	- Data Integrity and Authenticity can be compromised as message authentication codes and hashes are not used. - Data confidentiality can be compromised as data in memory can be accessed by a malicious user. - Denial of Service: DOS attacks are a possibility due to absence of application sessions and PKI validation policies. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount. - Unauthorized access: Due to the poor in-memory data handling policies, unauthorized access is a possibility after the attacker learns about the cryptographic keys from the memory. - Disclosure of sensitive information: Absence of data marking can lead to disclosure of sensitive information and IP data
Wireless Security	- Secure Wireless networking and security boundary controls are Implemented only when dealing with government projects. This can be a vulnerability during non-government projects. - Protected EAP is not implemented at my company. This	- Disclosure of sensitive information: As Secure Wireless networking and security boundary controls are not implemented for non-government projects, disclosure of sensitive data can be a possibility. - Data confidentiality can be compromised as secure tunneling

	method of tunneling the network communication can provide additional security. - My organization does not implement authorized architecture. This missing wireless risk management policy can lead to poor security of access points and bridges. Rogue access points and Evil twin access points can be easily be created. - Robust security network (RSN) is not implemented at my company. This can lead to poor authentication, encryption and key management services. - Wireless two-way email is not implemented at my organization. This can be a potential vulnerability.	method like PEAP in not used for network communication. - Denial of Service: DOS attacks are a possibility due to absence of RSN and authorized architecture. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount. - Unauthorized access: Due to the absence of RSN and authorized architecture, MAC address spoofing and sniffing attacks are possible which can lead to unauthorized access. - Data integrity and confidentiality can be compromised as wireless two-way email is not used.

Top 5 Asset Risks:

1. Vulnerabilities related to network related attacks
2. Deep packet inspection and hybrid technology firewalls are missing in my organization which play a key role in detection of trojans email viruses etc.
3. Signature-based, Anomaly-based or rule-based NIDS is not implemented and as a result the threat detection and analysis could not be performed effectively at the enclave gateways
4. The Time and Count limits on Network session parameters is not implemented in my organization. The most common time limit set for sessions in 10 min although Web Admins usually set it for 8 min.
5. In my company the data in memory is not cleared after its use. This may lead to range of vulnerabilities including data being read or altered by malicious users.

Top 5 Vulnerability Risks:

1. Disclosure of sensitive information
2. Unauthorized access: Due to the absence of network TAPs, data cannot be properly monitored and collected. This can lead to unauthorized access not being detected.
3. Disclosure of sensitive information: Attacks like eavesdropping can play a role in disclosure of information.

4. Denial of Service: DOS attacks are a possibility due to the absence of boundary defenses and recovery can be difficult due to missing controls like clustering and federation. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount.
5. Data Integrity and Authenticity can be compromised as message authentication codes and hashes are not used. Data confidentiality can be compromised as data in memory can be accessed by a malicious user.

9a. List of recommended Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the ranked vulnerability risks (it is not required to write detailed policies) – Risk Prevention Strategy

1. Logical Network Port Security should be implemented so that all the unnecessary ports can be closed and be less susceptible to attacks from the internet.
2. Implementation of deep packet inspection and hybrid firewall technologies is crucial as they can be able to detect malicious payload and prevent some critical cyber-attacks on the organization.
3. Signature-based, Anomaly-based or rule-based NIDS needs to be implemented to efficiently detect DOS attacks and other malware.
4. Implementing Time and Count limits on Network session parameters can greatly increase the security of the database while prevent many malicious attack attempts.
5. All the data in memory should be cleared after use and all the data should also be encrypted in memory when not in use

List of recommended Hardening methods and policies for critical assets that should be implemented to reduce ranked asset risk impact and thus mitigate the identified risks and increase resilience (it is not required to write detailed policies) – Risk Response Strategy

1. Data Activity Monitoring (DAM) solution can be implemented to closely monitor traffic and to avoid data leaks. An average hacker conducts reconnaissance six months before the actual breach, hence monitoring for unusual behavior can help deter a data breach.
2. Network TAPs and Data Activity Monitoring (DAM) solution can be implemented to closely monitor traffic and to avoid data leaks. An average hacker conducts reconnaissance six months before the actual breach, hence monitoring for unusual behavior can help deter a data breach
3. RSA key sizes should be increased to 4096 bits to safeguard against any possible attacks
4. It is good to implement clustering and federated databases to recover quickly against DOS attacks and reduce downtime.
5. Security controls like ACL's and permissions should be implemented for applications with excessive privileges.

10. Cybersecurity Workforce Risk Management Implementation

1. **List of Cybersecurity Specialty Areas that exist in your company (see NCWF, Appendix A2)**
2. **List of Cybersecurity Work Roles that exist in your company (see NCWF, Appendix A3)**

IA Specialty Areas	**IA Work Roles**
Risk Management (RSK)	Authorizing Official/Designating Representative
	Security Control Assessor
Software Development (DEV)	Security Control Assessor
	Secure Software Assessor
Technology R&D (TRD)	Research & Development Specialist
Systems Requirements Planning (SRP)	Systems Requirements Planner
Data Administration (ADTA)	Database Administrator
	Data Analyst
Customer Service and Technical Support (STS)	Technical Support Specialist
Network Services (NET)	Network Operations Specialist
Systems Administration (ADM)	System Administrator
Cybersecurity Management (MGT)	Information Systems Security Manager
	Communications Security (COMSEC) Manager
Cybersecurity Defense Analysis (CDA)	Cyber Defense Analyst
Incident Response (CIR)	Cyber Defense Incident Responder
Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst
Targets (TGT)	Target Network Analyst

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

- Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2)
- 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.
- Manage Accreditation Packages (e.g., ISO/IEC 15026-2).
- 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.

- Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.
- Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
- 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).
- Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.
- Assess the effectiveness of security controls.
- Assess all the configuration management (change configuration/release management) processes.
- Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.
- Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.
- Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.
- 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.
- Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.
- Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.
- Consult with engineering staff to evaluate interface between hardware and software.
- Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.
- Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.
- 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.
- Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
- 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.
- Review and validate data mining and data warehousing programs, processes, and requirements.
- Research current technology to understand capabilities of required system or network.

- Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.
- Collaborate with stakeholders to identify and/or develop appropriate solutions technology.
- Design and develop new tools/technologies as related to cybersecurity.
- Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.
- 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.
- Follow software and systems engineering life cycle standards and processes.
- Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases.
- Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities.
- Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.
- Conduct import/export reviews for acquiring systems and software.
- Develop data management capabilities (e.g., cloud-based, centralized cryptographic key management) to include support to the mobile workforce.
- Research and evaluate available technologies and standards to meet customer requirements.
- Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications.
- Consult with customers to evaluate functional requirements.
- Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions.
- Define project scope and objectives based on customer requirements.
- Develop and document requirements, capabilities, and constraints for design procedures and processes.
- Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements.
- Oversee and make recommendations regarding configuration management.
- Perform needs analysis to determine opportunities for new and improved business process solutions.
- Prepare use cases to justify the need for specific information technology (IT) solutions.
- Translate functional requirements into technical solutions.
- Develop and document supply chain risks for critical system elements, as appropriate.
- Develop and document User Experience (UX) requirements including information architecture and user interface requirements.
- Design and document quality standards.
- Document a system's purpose and preliminary system security concept of operations.
- Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware).
- Define baseline security requirements in accordance with applicable guidelines.
- Develop cost estimates for new or modified system(s).

- Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements.
- Analyze and plan for anticipated changes in data capacity requirements.
- Maintain database management systems software.
- 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.
- Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.
- 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.
- Implement data mining and data warehousing applications.
- Install and configure database management systems and software.
- Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
- Troubleshoot system hardware and software.
- Analyze incident data for emerging trends.
- Develop and deliver technical training to educate others or meet customer needs.
- Maintain incident tracking and solution database.
- Diagnose and resolve customer reported system incidents, problems, and events.
- 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.
- Administer accounts, network rights, and access to systems and equipment.
- Perform asset management/inventory of information technology (IT) resources.
- Monitor and report client-level computer system performance.
- Develop a trend analysis and impact report.
- 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 and maintain network infrastructure device operating system software (e.g., IOS, firmware).

- 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.
- Conduct functional and connectivity testing to ensure continuing operability.
- Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.
- Develop and document systems administration standard operating procedures.
- Maintain baseline system security according to organizational policies.
- Manage accounts, network rights, and access to systems and equipment.
- Plan, execute, and verify data redundancy and system recovery procedures.
- Provide ongoing optimization and problem-solving support.
- Install, update, and troubleshoot systems/servers.
- Check system hardware availability, functionality, integrity, and efficiency.
- Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.
- Comply with organization systems administration standard operating procedures.
- Implement and enforce local network usage policies and procedures.
- Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.
- Monitor and maintain system/server configuration.
- Oversee installation, implementation, configuration, and support of system components.
- Diagnose faulty system/server hardware.
- Perform repairs on faulty system/server hardware.
- Troubleshoot hardware/software interface and interoperability problems.
- Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
- Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.
- Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.
- Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.
- Ensure that security improvement actions are evaluated, validated, and implemented as required.
- Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy.
- Evaluate cost/benefit, economic, and risk analysis in decision-making process.
- Recognize a possible security violation and take appropriate action to report the incident, as required.

- Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
- Develop content for cyber defense tools.
- 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.
- Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.
- 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.
- Perform cyber defense trend analysis and reporting.
- 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.
- Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.
- Plan and recommend modifications or adjustments based on exercise results or system environment.
- Provide daily summary reports of network events and activity relevant to cyber defense practices.
- Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
- Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.
- Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.
- Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.
- Determine tactics, techniques, and procedures (TTPs) for intrusion sets.
- Examine network topologies to understand data flows through the network.
- Recommend computing environment vulnerability corrections.
- Identify and analyze anomalies in network traffic using metadata.
- Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).
- Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.
- Isolate and remove malware.
- Identify applications and operating systems of a network device based on network traffic.
- 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.

- 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.
- Analyze and report organizational security posture trends.
- Analyze and report system security posture trends.
- Assess adequate access controls based on principles of least privilege and need-to-know.
- 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.
- Assess and monitor cybersecurity related to system implementation and testing practices.
- Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.
- Work with stakeholders to resolve computer security incidents and vulnerability compliance.
- Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
- 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 cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
- Perform cyber defense trend analysis and reporting.
- Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
- 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).
- Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
- Track and document cyber defense incidents from initial detection through final resolution.
- Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.
- 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.
- Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.
- Coordinate with intelligence analysts to correlate threat assessment data.
- Provide actionable recommendations to critical stakeholders based on data analysis and findings.

- 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.
- Coordinate incident response functions.
- Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
- Conduct and/or support authorized penetration testing on enterprise network assets.
- 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.
- Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).
- 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).
- Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).
- Provide expertise to course of action development.
- Classify documents in accordance with classification guidelines.
- Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.
- Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.
- Identify and conduct analysis of target communications to identify information essential to support operations.
- Conduct nodal analysis.
- Conduct quality control to determine validity and relevance of information gathered about networks.
- Conduct target research and analysis.
- Determine what technologies are used by a given target.
- Apply analytic techniques to gain more target information.
- 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.)
- Generate requests for information.
- Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.
- Identify collection gaps and potential collection strategies against targets.
- Identify network components and their functionality to enable analysis and target development.
- Make recommendations to guide collection in support of customer requirements.

- Provide subject matter expertise to development of exercises.
- Perform content and/or metadata analysis to meet organization objectives.
- Profile targets and their activities.
- Provide target recommendations which meet leadership objectives.
- Review appropriate information sources to determine validity and relevance of information gathered.
- 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.

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

NICE Specialty Area	Status
Risk Management (RSK)	Present
Software Development (DEV)	Present
Systems Architecture (ARC)	Absent
Technology R&D (TRD)	Present
Systems Requirements Planning (SRP)	Present
Test and Evaluation (TST)	Absent
Systems Development (SYS)	Absent
Data Administration (DTA)	Present
Knowledge Management (KMG)	Absent
Customer Service and Technical Support (STS)	Present
Network Services (NET)	Present
Systems Administration (ADM)	Present
Systems Analysis (ANA)	Absent
Legal Advice and Advocacy (LGA)	Absent
Training, Education, and Awareness (TEA)	Absent
Cybersecurity Management (MGT)	Present
Strategic Planning and Policy (SPP)	Absent
Executive Cyber Leadership (EXL)	Absent
Program/Project Management (PMA) and Acquisition	Absent
Cybersecurity Defense Analysis (CDA)	Present
Cybersecurity Defense Infrastructure Support (INF)	Absent
Incident Response (CIR)	Present
Vulnerability Assessment and Management (VAM)	Present
Threat Analysis (TWA)	Absent
Exploitation Analysis (EXP)	Absent
All-Source Analysis (ASA)	Absent
Targets (TGT)	Present
Language Analysis (LNG)	Absent

Collection Operations (CLO)	Absent
Cyber Operational Planning (OPL)	Absent
Cyber Operations (OPS)	Absent
Cyber Investigation (INV)	Absent
Digital Forensics (FOR)	Absent

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

Work Role	**Status**
Authorizing Official/Designating Representative	Present
Security Control Assessor	Present
Software Developer	Present
Secure Software Assessor	Absent
Enterprise Architect	Absent
Security Architect	Absent
Research & Development Specialist	Present
Systems Requirements Planner	Present
System Testing and Evaluation Specialist	Absent
Information Systems Security Developer	Absent
Systems Developer	Absent
Database Administrator	Present
Data Analyst	Absent
Knowledge Manager	Absent
Technical Support Specialist	Present
Network Operations Specialist	Present
System Administrator	Present
Systems Security Analyst	Absent
Cyber Legal Advisor	Absent
Privacy Officer/Privacy Compliance Manager	Absent
Cyber Instructional Curriculum Developer	Absent
Cyber Instructor	Absent
Information Systems Security Manager	Absent
Communications Security (COMSEC) Manager	Present
Cyber Workforce Developer and Manager	Absent
Cyber Policy and Strategy Planner	Absent
Executive Cyber Leadership	Absent
Program Manager	Absent
IT Project Manager	Absent
Product Support Manager	Absent
IT Investment/Portfolio Manager	Absent
IT Program Auditor	Absent
Cyber Defense Analyst	Present
Cyber Defense Infrastructure Support Specialist	Absent
Cyber Defense Incident Responder	Present

Vulnerability Assessment Analyst	Present
Threat/Warning Analyst	Absent
Exploitation Analyst	Absent
All-Source Analyst	Absent
Mission Assessment Specialist	Absent
Target Developer	Absent
Target Network Analyst	Present
Multi-Disciplined Language Analyst	Absent
All Source-Collection Manager	Absent
All Source-Collection Requirements Manager	Absent
Cyber Intel Planner	Absent
Cyber Ops Planner	Absent
Partner Integration Planner	Absent
Cyber Operator	Absent
Cyber Crime Investigator	Absent
Law Enforcement /Counter Intelligence Forensics Analyst	Absent
Cyber Defense Forensics Analyst	Absent

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

Work Roles	**Tasks**	**Status**
Authorizing Official/Designating Representative	- Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2) - 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. - Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	Present
Security Control Assessor	- Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). - Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks. - Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network. - Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.	Present

	- Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data - Establish acceptable limits for the software application, network, or system. - Manage Accreditation Packages (e.g., ISO/IEC 15026-2). - Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. - Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. - 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. - Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk. - Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. - 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). - Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	

	- Assess the effectiveness of security controls. - Approve all the configuration management (change configuration/release management) processes.	
Software Developer	- Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application. - Analyze user needs and software requirements to determine feasibility of design within time and cost constraints. - Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support. - 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. - Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program. - Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces. - Consult with engineering staff to evaluate interface between hardware and software. - Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced. - Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design. - 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.	Present

	- 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. - Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. - 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.	
Secure Software Assessor	- 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. - Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration. - Identify basic common coding flaws at 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 risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes	Absent

	a major change. - 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. - Perform penetration testing as required for new or updated 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. - 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. - Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct. - 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. - Determine and document software patches or the extent of releases that would leave software vulnerable.	
Enterprise Architect	- 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,	Absent

	backup requirements, and material supportability requirements for system recover/restoration. - Employ secure configuration management processes. - Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. - Identify and prioritize critical business functions in collaboration with organizational stakeholders. - Provide advice on project costs, design concepts, or design changes. - 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). - 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. - 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. - Write detailed functional specifications that document the architecture development process. - Analyze user needs and requirements to plan architecture. - Capture and integrate essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. - Develop enterprise architecture or system components required to meet user needs. - Document and update as necessary all definition and architecture activities. - Integrate results regarding the identification of gaps in security architecture. - Plan implementation strategy to ensure that enterprise components can be integrated and aligned. - Translate proposed capabilities into technical requirements. - Review and approve a supply chain security/risk management policy. - Integrate key management functions as related to cyberspace.	
Security Architect		Absent

	- Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. - 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. - 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 (eel., UNCLASSIFIED, SECRET, and TOP SECRET). - Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle. - Employ secure configuration management processes. - Ensure that acquired or developed system(s) and architecture(s) are consistent with organization 's cybersecurity architecture guidelines. - 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. - Provide advice on project costs, design concepts, or design changes. - Provide input on security requirements to be included in statements of work and other appropriate procurement documents. - 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). - Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. - 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. - 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. - Write detailed functional specifications that document the architecture development process. - 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. - Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately. - Translate proposed capabilities into technical requirements. - Assess and design security management functions as related to cyberspace.	
Research & Development Specialist	- Review and validate data mining and data warehousing programs, processes, and requirements. - Research current technology to understand capabilities of required system or network. - Identify cyber capabilities strategies for custom hardware and software development based on mission requirements. - Collaborate with stakeholders to identify and/or develop appropriate solutions technology. - Design and develop new tools/technologies as related to cybersecurity. - Evaluate network infrastructure vulnerabilities to enhance capabilities being developed. - Follow software and systems engineering life cycle standards and processes. - Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases. - Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities. - Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.	Present

	- Develop data management capabilities (e.g., cloud-based, centralized cryptographic key management) to include support to the mobile workforce. - Research and evaluate available technologies and standards to meet customer requirements.	
Systems Requirements Planner	- Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications. - Consult with customers to evaluate functional requirements. - Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions. - Define project scope and objectives based on customer requirements. - Develop and document requirements, capabilities, and constraints for design procedures and processes. - Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements. - Oversee and make recommendations regarding configuration management. - Perform needs analysis to determine opportunities for new and improved business process solutions. - Prepare use cases to justify the need for specific information technology (IT) solutions. - Translate functional requirements into technical solutions. - Develop and document supply chain risks for critical system elements, as appropriate. - Develop and document User Experience (UX) requirements including information architecture and user interface requirements. - Design and document quality standards. - Document a system's purpose and preliminary system security concept of operations. - Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware). - Define baseline security requirements in accordance with applicable guidelines. - Develop cost estimates for new or modified system(s). - Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements.	Present
System Testing and Evaluation Specialist	- Determine level of assurance of developed capabilities based on test results.	Absent

	- Develop test plans to address specifications and requirements. - Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). - Make recommendations based on test results. - Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated. - Create auditable evidence of security measures. - Validate specifications and requirements for testability. - 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. - Record and manage test data.	
Information Systems Security Developer	- Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support. - Apply security policies to applications that interface with one another, such as Business-to-Business (828) applications. - Assess the effectiveness of cybersecurity measures utilized by system(s). - Assess threats and vulnerabilities of computer system(s) to develop a security risk profile. - Build, test, and modify product prototypes using working models or theoretical models. - 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 - Design and develop cybersecurity or cybersecurity-enabled products. - Design hardware, operating systems, and software applications to adequately address cybersecurity requirements. - 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.	Absent

	- Develop and direct system testing and validation procedures and documentation. - Develop detailed security design documentation for component and interface specifications to support system design and development. - Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. - Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed. - Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications. - Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements. - 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). - 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. - Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products follow organization's evaluation and validation requirements. - Implement security designs for new or existing system(s). - Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts). - Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. - Provide guidelines for implementing developed systems to customers or installation teams.	

	- 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). - Store, retrieve, and manipulate data for analysis of system capabilities and requirements. - Provide support to security/certification test and evaluation activities. - Utilize models and simulations to analyze or predict system performance under different operating conditions. - Design and develop key management functions (as related to cybersecurity). - 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). - Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary. - Implement and integrate system development life cycle (SDLC) methodologies (e.g., 18M Rational unified Process) into development environment. - Employ configuration management processes. - Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies. - 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. - Develop mitigation strategies to address cost, schedule, performance, and security risks. - Perform an information security risk assessment. - Perform security reviews and Identify security gaps in architecture.	

	- Provide input to implementation plans and standard operating procedures as they relate to information systems security. - Trace system requirements to design components and perform gap analysis. - Verify stability, interoperability, portability, and/or scalability of system architecture.	
Systems Developer	- Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life build, test, and modify product prototypes using working models or theoretical models - Design and develop cybersecurity or cybersecurity enabled products - 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. - Develop and direct system testing and validation procedures and documentation - Develop architectures or system components consistent with technical specifications - Develop Disaster Recover-v 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 identify and find work-arounds for communication protocols that are not - Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recover after a system failure or during a system recover'/ event based on overall system requirements for continuity and availability - 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 - Perform risk analysis (24, threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change	Absent

	- Provide guidelines for implementing developed systems to customers or installation teams - Provide input to the Risk Management Framework process activities and related documentation system life—cycle support plans, concept of operations, operational procedures, and maintenance training - Store, retrieve, and manipulate data for analysis of system capabilities and requirements - Utilize models and simulations to analyze or predict system performance under different operating - Implement and integrate system development life cycle (SDLC) methodologies 13M Rational Unified - Process) into development environment - Employ configuration management processes - 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 - Design and develop system administration and management functionality for privileged access users - Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies - Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle - Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary - Design hardware, operating systems, and software applications to adequately address requirements - Design to security requirements to ensure requirements are met for all systems and/or applications - Develop detailed design documentation for component and interface specifications to support system design and development - Develop mitigation strategies to address cost, schedule, performance, and security risks - Identify components or elements, allocate comprehensive functional components to include security	

	functions, and describe the relationships between the elements - Implement designs for new or existing system(s) - Perform security reviews and identify security gaps in architecture - Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials - Provide support to test and evaluation activities. - Trace system requirements to design components and perform gap analysis. - Verify stability, interoperability, portability, and/or scalability of system architecture. - Analyze user needs and requirements to plan and conduct system development. - 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).	
Database Administrator	- Analyze and plan for anticipated changes in data capacity requirements. - Maintain database management systems software. - 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. - Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.	Present

	- 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. - Implement data mining and data warehousing applications. - Install and configure database management systems and software.	
Data Analyst	- Analyze and define data requirements and specifications. - Analyze and plan for anticipated changes in data capacity requirements. - Develop data standards, policies, and procedures. - Manage the compilation, cataloging, caching, distribution, and retrieval of data. - Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. - Provide recommendations on new database technologies and architectures. - Analyze data sources to provide actionable recommendations. - Assess the validity of source data and subsequent findings. - Collect metrics and trending data. - Conduct hypothesis testing using statistical processes. - Confer with systems analysts, engineers, programmers, and others to design application. - Develop and facilitate data-gathering methods. - Develop strategic insights from large data sets. - Present technical information to technical and nontechnical audiences. - Present data in creative formats. - Program custom algorithms. - Provide actionable recommendations to critical stakeholders based on data analysis and findings. - Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method. - Effectively allocate storage capacity in the design of data management systems.	Present

	- 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). - Utilize different programming languages to write code, open files, read files, and write output to different files. - 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). - Develop and implement data mining and data warehousing programs.	
Knowledge Manager	- Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users. - Develop an understanding of the needs and requirements of information end-users. - Monitor and report the usage of knowledge management assets and resources. - Plan and manage the delivery of knowledge management projects. - Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information. - Lead efforts to promote the organization's use of knowledge management and information sharing. - Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files). - Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization's intellectual capital. - Promote knowledge sharing between information owners/users through an organization's operational processes and systems.	Absent
Technical Support Specialist	- Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). - Troubleshoot system hardware and software. - Analyze incident data for emerging trends. - Develop and deliver technical training to educate others or meet customer needs.	Present

	- Maintain incident tracking and solution database. - Diagnose and resolve customer reported system incidents, problems, and events. - 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. - Administer accounts, network rights, and access to systems and equipment. - Perform asset management/inventory of information technology (IT) resources. - Monitor and report client-level computer system performance. - Develop a trend analysis and impact report.	
Network Operations Specialist	- 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 and maintain network infrastructure device operating system software (e.g., IOS, firmware). - 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.	Present
System Administrator	- Conduct functional and connectivity testing to ensure continuing operability. - Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs. - Develop and document systems administration standard operating procedures. - Maintain baseline system security according to organizational policies. - Manage accounts, network rights, and access to systems and equipment. - Plan, execute, and verify data redundancy and system recovery procedures.	Present

	- Provide ongoing optimization and problem-solving support. - Install, update, and troubleshoot systems/servers. - Check system hardware availability, functionality, integrity, and efficiency. - Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing. - Comply with organization systems administration standard operating procedures. - Implement and enforce local network usage policies and procedures. - Manage system/server resources including performance, capacity, availability, serviceability, and recoverability. - Monitor and maintain system/server configuration. - Oversee installation, implementation, configuration, and support of system components. - Diagnose faulty system/server hardware. - Perform repairs on faulty system/server hardware. - Troubleshoot hardware/software interface and interoperability problems.	
Systems Security Analyst	- Apply security policies to meet security objectives of the system. - Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. - Ensure all systems security operations and maintenance activities are properly documented and updated. - 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. - Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. - 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	Absent

	- requirements for the operational environment of the system. - Perform cybersecurity testing of developed applications and/or systems. - Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. - Plan and recommend modifications or adjustments based on exercise results or system environment. - Properly document all systems security implementation, operations, and maintenance activities and update as necessary. - Provide cybersecurity guidance to leadership. - 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. - Assess the effectiveness of security controls. - Assess all the configuration management (change configuration/release management) processes. - Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements. - Analyze and report organizational security posture trends. - Analyze and report system security posture trends. - 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 security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or - system components as needed. - Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. - Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment. - 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. - Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities. - Work with stakeholders to resolve computer security incidents and vulnerability compliance. - Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	
Cyber Legal Advisor	- Advocate organization's official position in legal and legislative proceedings. - Evaluate contracts to ensure compliance with funding, legal, and program requirements. - Evaluate the effectiveness of laws, regulations, policies, standards, or procedures. - Interpret and apply laws, regulations, policies, standards, or procedures to specific issues. - Resolve conflicts in laws, regulations, policies, standards, or procedures. - Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances. - Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance. - Develop guidelines for implementation. - 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. - Evaluate the impact of changes to laws, regulations, policies, standards, or procedures. - Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients. - Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures. - Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).	Absent
Privacy Officer/Privacy	- Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Absent

Compliance Manager	- Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. - Conduct functional and connectivity testing to ensure continuing operability. - Establish a risk management strategy for the organization that includes a determination of risk tolerance. - 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). - Develop and maintain strategic plans. - Evaluate contracts to ensure compliance with funding, legal, and program requirements. - Evaluate cost/benefit, economic, and risk analysis in decision-making process. - Interpret and apply laws, regulations, policies, standards, or procedures to specific issues. - Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program. - Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions. - Present technical information to technical and nontechnical audiences. - 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. - Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients. - Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations. - 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.	

	- 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. - Liaise with regulatory and accrediting bodies. - Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues. - 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. - Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required. - Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required. - Work with business teams and senior management to ensure awareness of "best practices" on privacy and data security Issues. - Work with organization senior management to establish an organization-wide Privacy Oversight Committee Serve in a leadership role for Privacy Oversight Committee activities - Collaborate on cyber privacy and security policies and procedures - Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation - 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 - Provide strategic guidance to corporate officers regarding information resources and technology - Assist the Security Officer with the development and implementation of an information infrastructure - Coordinate with the Corporate Compliance Officer regarding procedures for documenting and reporting self-disclosures of any evidence of privacy violations. - Work cooperatively with applicable organization units in overseeing consumer information access rights	

	- Serve as the information privacy liaison for users of technology systems - Act as a liaison to the information systems department - Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations - 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 - Conduct on-going privacy training and awareness activities - 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 - 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. - Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee - Work with External Affairs to respond to press and other inquiries regarding concern over consumer and employee data - Provide leadership for the organization's privacy program - Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization - 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	

	- Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures - Resolve allegations of noncompliance with the corporate privacy policies or notice of information practices - Develop and coordinate a risk management and compliance framework for privacy	
Cyber Instructional Curriculum Developer	- - Support the design and execution of exercise scenarios. - Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce. - Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. - Research current technology to understand capabilities of required system or network. - Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction. - Conduct learning needs assessments and identify requirements. - Create interactive learning exercises to create an effective learning environment. - Develop or assist in the development of training policies and protocols for cyber training. - Develop the goals and objectives for cyber curriculum. - 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. - Correlate training and learning to business or mission requirements. - Create training courses tailored to the audience and physical environment. - Design training curriculum and course content based on requirements. - Participate in development of training curriculum and course content. - Conduct periodic reviews/revisions of course content for accuracy, completeness alignment, and currency (e.g., course	Absent

	- content documents, lesson plans, student texts, examinations, schedules of instruction, and course descriptions). - Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media). - 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.	
Cyber Instructor	- Conduct interactive training exercises to create an effective learning environment. - Develop new or identify existing awareness and training materials that are appropriate for intended audiences. - Evaluate the effectiveness and comprehensiveness of existing training programs. - Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, - Schedules of Instruction [SOI], and course descriptions). - Support the design and execution of exercise scenarios. - Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce. - Develop or assist in the development of computer-based training modules or classes. - Develop or assist in the development of course assignments. - Develop or assist in the development of course evaluations. - Develop or assist in the development of grading and proficiency standards. - Assist in the development of individual/collective development, training, and/or remediation plans. - Develop or assist in the development of learning objectives and goals. - Develop or assist in the development of on-the-job training materials or programs. - Develop or assist in the development of written tests for measuring and assessing learner proficiency. - Conduct learning needs assessments and identify requirements.	Absent

	- Develop or assist in the development of training policies and protocols for cyber training. - Develop the goals and objectives for cyber curriculum. - Present technical information to technical and nontechnical audiences. - Present data in creative formats. - Write and publish after action reviews. - Deliver training courses tailored to the audience and physical/virtual environments. - Apply concepts, procedures, software, equipment, and/or technology applications to students. - Design training curriculum and course content based on requirements. - Participate in development of training curriculum and course content. - Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness. - Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for the most effective learning environment. - Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses). - Recommend revisions to curriculum and course content based on feedback from previous training sessions. - Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media). - 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.	
Information Systems Security Manager	- To support information technology (IT) security goals and objectives and reduce overall organizational risk. - Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program. - Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Absent

	- Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. - Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture. - Collect and maintain data needed to meet system cybersecurity reporting. - Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. - Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. - Ensure that security improvement actions are evaluated, validated, and implemented as required. - Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment. - Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s). - Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture. - Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy. - Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed. - Evaluate cost/benefit, economic, and risk analysis in decision-making process. - Identify alternative information security strategies to address organizational security objective. - Identify information technology (IT) security program implications of new technologies or technology upgrades. - 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. - Interpret and/or approve security requirements relative to the capabilities of new information technologies.	

	- Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program. - Lead and align information technology (IT) security priorities with the security strategy. - Lead and oversee information security budget, staffing, and contracting. - Manage the monitoring of information security data sources to maintain organizational situational awareness. - Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst - Reports, NTSM, MTOs) for the enterprise constituency. - Manage threat or target analysis of cyber defense information and production of threat information within the enterprise. - Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. - Oversee the information security training and awareness program. - Participate in an information security risk assessment during the Security Assessment and Authorization process. - Participate in the development or modification of the computer environment cybersecurity program plans and requirements. - Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations. - Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. - 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 - Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.	

	- Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters. - Recognize a possible security violation and take appropriate action to report the incident, as required. - Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements. - Recommend policy and coordinate review and approval. - Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. - Track audit findings and recommendations to ensure that appropriate mitigation actions are taken. - Use federal and organization-specific published documents to manage operations of their computing environment system(s). - Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. - Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies. - Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk. - Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. - Identify security requirements specific to an information technology (IT) system in all phases of the system life - Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. - 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.	

Communications Security (COMSEC) Manager	- Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture. - Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. - Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. - Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. - Ensure that security improvement actions are evaluated, validated, and implemented as required. - Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy. - Evaluate cost/benefit, economic, and risk analysis in decision-making process. - Recognize a possible security violation and take appropriate action to report the incident, as required. - Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Absent
Cyber Workforce Developer and Manager	- Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to sort Information technology, security goals and objectives and reduce overall or organizational risk. - Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, stems, and elements. - Communicate the value of information technology - security throughout all levels of the organization stakeholders. - Collaborate With stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. - Development programs, and guidelines for implementation. - Establish and maintain communication channels with stakeholders. - Evaluate cost/benefit, economic, and risk anal sis in decision-making. - Review existing policies with stakeholders.	Absent

	- Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials. - Conduct learning needs assessments and identify requirements. - Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards. - Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human critical assets. - Develop and implement standardized situation descriptions based on established work roles. - Develop and review recruiting , hiring , and retention procedures in accordance with current HR policies. - Develop cyber career field classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers. - Develop or assist in the development of training policies and protocols for better training. - Ensure that career fields are maintained in accordance with organizational HR policies and directives. - Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity , diverse , and fair hiring /employment practices. - Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of situations identified, filled, and filled with qualified personnel. - Establish and oversee waiver processes for cyber career field entry and training qualification requirements. - Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields. - Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements. - Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational	

	requirements. - 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. - Review and apply cyber career field qualification standards. - Review and apply organizational policies related to or influencing the cyber workforce. - Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards. - Support integration of qualified cyber workforce personnel into information systems life cycle development processes. - Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy. - Analyze organizational cyber policy. - Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. - Correlate training and learning to business or mission requirements. - Define and integrate current and future mission environments. - Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan. - Draft, staff, and publish cyber policy. - 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. - Seek consensus on proposed policy changes from stakeholders. - Provide policy guidance to cyber management, staff, and users. - Review, conduct, or participate in audits of cyber programs and projects. - Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media). - Support the CIO in the formulation of cyber-related policies.	

	- Review and approve a supply chain security/risk management policy.	
Cyber Policy and Strategy Planner	- Develop policy, programs, and guidelines for implementation. - Establish and maintain communication channels with stakeholders. - Review existing and proposed policies with stakeholders. - Serve on agency and interagency policy boards. - Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials. - Ensure that cyber workforce management policies and processes comply with legal and organizational requirements - regarding equal opportunity, diversity, and fair hiring/employment practices. - 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. - Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards. - Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy. - Analyze organizational cyber policy. - Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. - Define and integrate current and future mission environments. - Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan. - Draft, staff, and publish cyber policy. - Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services. - Seek consensus on proposed policy changes from stakeholders. - Provide policy guidance to cyber management, staff, and users. - Review, conduct, or participate in audits of cyber programs and projects.	Absent

	- Support the CIO in the formulation of cyber-related policies.	
Executive Cyber Leadership	- 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. - Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program. - Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. - Advocate organization's official position in legal and legislative proceedings. - Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. - Develop and maintain strategic plans. - Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector - General) to ensure appropriate and accurate dissemination of incident and another Computer Network Defense - Lead and align information technology (IT) security priorities with the security strategy. - Lead and oversee information security budget, staffing, and contracting. - Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst - Reports, NTSM, MTOs) for the enterprise constituency. - Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. - Recommend policy and coordinate review and approval. - Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. - Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Absent

	- Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. - Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies. - Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle. - Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	
Program Manager	- Develop and maintain strategic plans. - Develop methods to monitor and measure risk, compliance, and assurance efforts. - Perform needs analysis to determine opportunities for new and improved business process solutions. - Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. - Resolve conflicts in laws, regulations, policies, standards, or procedures. - Review or conduct audits of information technology (IT) programs and projects. - Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. - Develop and document supply chain risks for critical system elements, as appropriate. - Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. - Develop contract language to ensure supply chain, system, network, and operational security are met. - 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. - Coordinate and manage the overall service provided to a customer end-to-end. - Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Present

	- Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs). - Participate in the acquisition process as necessary. - Conduct import/export reviews for acquiring systems and software. - 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. - Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training). - Lead and oversee budget, staffing, and contracting. - Draft and publish supply chain security and risk management documents.	
IT Project Manager	- Develop methods to monitor and measure risk, compliance, and assurance efforts. - Perform needs analysis to determine opportunities for new and improved business process solutions. - Provide advice on project costs, design concepts, or design changes. - Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. - Provide ongoing optimization and problem-solving support. - Provide recommendations for possible improvements and upgrades. - Resolve conflicts in laws, regulations, policies, standards, or procedures. - Review or conduct audits of information technology (IT) programs and projects. - Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. - Develop and document supply chain risks for critical system elements, as appropriate. - Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. - Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction	Absent

	and monitor all significant activities so the service is delivered successfully. - Coordinate and manage the overall service provided to a customer end-to-end. - 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. - Gather feedback on customer satisfaction and internal service performance to foster continual improvement. - Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs). - Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up. - Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives. - Participate in the acquisition process as necessary. - Conduct import/export reviews for acquiring systems and software. - 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. - Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training). - Lead and oversee budget, staffing, and contracting. - Draft and publish supply chain security and risk management documents.	
Product Support Manager	- Develop methods to monitor and measure risk, compliance, and assurance efforts. - Perform needs analysis to determine opportunities for new and improved business process solutions. - Provide advice on project costs, design concepts, or design changes. - Provide input to implementation plans and standard operating procedures. - Provide ongoing optimization and problem-solving support.	Present

	- Provide recommendations for possible improvements and upgrades. - Resolve conflicts in laws, regulations, policies, standards, or procedures. - Review or conduct audits of information technology (IT) programs and projects. - Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. - Develop and document supply chain risks for critical system elements, as appropriate. - Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. - Develop contract language to ensure supply chain, system, network, and operational security are met. - 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. - Coordinate and manage the overall service provided to a customer end-to-end. - 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. - Gather feedback on customer satisfaction and internal service performance to foster continual improvement. - Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up. - Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives. - Conduct import/export reviews for acquiring systems and software. - Develop supply chain, system, network, performance, and cybersecurity requirements. - Lead and oversee budget, staffing, and contracting. - Provide enterprise cybersecurity and supply chain risk management guidance.	

	- Draft and publish supply chain security and risk management documents. - Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	
IT Investment/Portfolio Manager	- Resolve conflicts in laws, regulations, policies, standards, or procedures. - Review or conduct audits of information technology (IT) programs and projects. - Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. - Develop contract language to ensure supply chain, system, network, and operational security are met. - Gather feedback on customer satisfaction and internal service performance to foster continual improvement. - Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. - Lead and oversee budget, staffing, and contracting. - Draft and publish supply chain security and risk management documents.	Present
IT Program Auditor	- Develop methods to monitor and measure risk, compliance, and assurance efforts. - Provide ongoing optimization and problem-solving support. - Provide recommendations for possible improvements and upgrades. - Review or conduct audits of information technology (IT) programs and projects. - Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. - Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up. - Conduct import/export reviews for acquiring systems and software. - Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Absent
Cyber Defense Analyst	- Develop content for cyber defense tools. - Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	Absent

	- Coordinate with enterprise-wide cyber defense staff to validate network alerts. - Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. - 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. - Perform cyber defense trend analysis and reporting. - 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. - Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. - Plan and recommend modifications or adjustments based on exercise results or system environment. - Provide daily summary reports of network events and activity relevant to cyber defense practices. - Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts. - Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities. - Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity. - Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information. - Determine tactics, techniques, and procedures (TTPs) for intrusion sets. - Examine network topologies to understand data flows through the network. - Recommend computing environment vulnerability corrections. - Identify and analyze anomalies in network traffic using metadata. - Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings). - Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools. - Isolate and remove malware.	

	- Identify applications and operating systems of a network device based on network traffic. - 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. - 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. - Analyze and report organizational security posture trends. - Analyze and report system security posture trends. - Assess adequate access controls based on principles of least privilege and need-to-know. - 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. - Assess and monitor cybersecurity related to system implementation and testing practices. - Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities. - Work with stakeholders to resolve computer security incidents and vulnerability compliance. - Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	
Cyber Defense Infrastructure Support Specialist	- 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.	Absent

	- Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources. - Build, install, configure, and test dedicated cyber defense hardware. - Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure. - Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s). - Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems). - Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization). - 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.	
Cyber Defense Incident Responder	- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. - 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 cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation. - Perform cyber defense trend analysis and reporting. - Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems. - 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). - Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Absent

	- Track and document cyber defense incidents from initial detection through final resolution. - Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies. - 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. - Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. - Coordinate with intelligence analysts to correlate threat assessment data. - Provide actionable recommendations to critical stakeholders based on data analysis and findings. - 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. - Coordinate incident response functions.	
Vulnerability Assessment Analyst	- Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives. - Conduct and/or support authorized penetration testing on enterprise network assets. - 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. - Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews). - 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	Absent

	environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). - Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).	
Threat/Warning Analyst	- Answer requests for information. - Provide subject matter expertise to the development of a common operational picture. - Maintain a common intelligence picture. - Provide subject matter expertise to the development of cyber operations specific indicators. - Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. - Assist in the identification of intelligence collection shortfalls. - Brief threat and/or target current situations. - Collaborate with intelligence analysts/targeting organizations involved in related areas. - Conduct in-depth research and analysis. - Conduct nodal analysis. - Develop information requirements necessary for answering priority information requests. - Evaluate threat decision-making processes. - Identify threats to Blue Force vulnerabilities. - Generate requests for information. - Identify threat tactics, and methodologies. - Identify intelligence gaps and shortfalls. - Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. - Monitor and report on validated threat activities. - Monitor open source websites for hostile content directed towards organizational or partner interests. - Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements. - Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies). - Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. - Provide current intelligence support to critical internal/external stakeholders as appropriate.	Present

	- Provide evaluation and feedback necessary for improving intelligence production, intelligence repotting, collection requirements, and operations. - 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. - Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities. - Report intelligence-derived significant network events and intrusions. - Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	
Exploitation Analyst	- Conduct and/or support authorized penetration testing on enterprise network assets. - Perform penetration testing as required for new or updated applications. - Apply and utilize authorized cyber capabilities to enable access to targeted networks. - Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements. - Apply and obey applicable statutes, laws, regulations and policies. - Perform analysis for target infrastructure exploitation activities. - Collaborate with other internal and external partner organizations on target access and operational issues. - Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers. - Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access. - Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access.	Absent

	- Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities. - Examine intercept-related metadata and content with an understanding of targeting significance. - Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development. - Identify gaps in our understanding of target technology and developing innovative collection approaches. - Identify, locate, and track targets via geospatial analysis techniques. - Lead or enable exploitation operations in support of organization objectives and target requirements. - Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications. - 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.	
All-Source Analyst	- Answer requests for information. - Provide expertise to course of action development. - Provide subject matter expertise to the development of a common operational picture. - Maintain a common intelligence picture. - Provide subject matter expertise to the development of cyber operations specific indicators. - Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. - Assist in the identification of intelligence collection shortfalls. - Brief threat and/or target current situations. - Collaborate with intelligence analysts/targeting organizations involved in related areas. - Conduct in-depth research and analysis. - Conduct nodal analysis. - Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology. - Develop information requirements necessary for answering priority information requests.	Absent

	- Engage customers to understand customers' intelligence needs and wants. - Evaluate threat decision-making processes. - Identify threat vulnerabilities. - Identify threats to Blue Force vulnerabilities. - Generate requests for information. - Identify threat tactics, and methodologies. - Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. - Identify and submit intelligence requirements for the purposes of designating priority information requirements. - Identify intelligence gaps and shortfalls. - Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to - designated cyber operations warning problem sets. - Monitor and report on validated threat activities. - Monitor open source websites for hostile content directed towards organizational or partner interests. - Monitor operational environment and report on adversarial activities which fulfill leadership's priority information - requirements. - Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies). - Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. - Provide subject matter expertise to website characterizations. - Provide analyses and support for effectiveness assessment. - Provide current intelligence support to critical internal/external stakeholders as appropriate. - Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations. - 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 input and assist in post-action effectiveness assessments. - Provide input and assist in the development of plans and guidance. - Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations. - Provide target recommendations which meet leadership objectives. - Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities. - Report intelligence-derived significant network events and intrusions. - Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	
Mission Assessment Specialist	- Provide expertise to course of action development. - Provide subject matter expertise to the development of a common operational picture. - Provide subject matter expertise to the development of cyber operations specific indicators. - Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. - Provide expertise to the development of measures of effectiveness and measures of performance. - Assist in the identification of intelligence collection shortfalls. - Brief threat and/or target current situations. - Collaborate with intelligence analysts/targeting organizations involved in related areas. - Conduct end-of-operations assessments. - Conduct in-depth research and analysis. - Conduct nodal analysis. - Conduct target research and analysis. - Develop information requirements necessary for answering priority information requests. - Develop measures of effectiveness and measures of performance. - Develop munitions effectiveness assessment or operational assessment materials. - Engage customers to understand customers' intelligence needs and wants. - Estimate operational effects generated through cyber activities.	Absent

	- Evaluate threat decision-making processes. - Identify threat vulnerabilities. - Generate requests for information. - Identify intelligence gaps and shortfalls. - Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. - Monitor and report on validated threat activities. - Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements. - Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., - threat assessments, briefings, intelligence studies, country studies). - Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. - Provide analyses and support for effectiveness assessment. - Provide current intelligence support to critical internal/external stakeholders as appropriate. - Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations. - 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 input and assist in post-action effectiveness assessments. - Provide input and assist in the development of plans and guidance. - Provide effectiveness support to designated exercises, and/or time sensitive operations. - Provide target recommendations which meet leadership objectives. - Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	
Target Developer	- Accurately characterize targets. - Provide expertise to course of action development.	Absent

	- Provide expertise to the development of measures of effectiveness and measures of performance. - Build and maintain electronic target folders. - Collaborate with intelligence analysts/targeting organizations involved in related areas. - Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas. - Conduct nodal analysis. - Conduct target research and analysis. - Coordinate target vetting with appropriate partners. - Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology. - Determine what technologies are used by a given target. - Develop all-source intelligence targeting materials. - Develop measures of effectiveness and measures of performance. - Develop munitions effectiveness assessment or operational assessment materials. - Estimate operational effects generated through cyber activities. - Evaluate available capabilities against desired effects to recommend efficient solutions. - Generate requests for information. - Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. - Identify critical target elements. - Initiate requests to guide tasking and assist with collection management. - Maintain target lists (i.e., RT L, JTL, CT L, etc.). - Perform targeting automation activities. - Characterize websites. - Produce target system analysis products. - Provide aim point and reengagement recommendations. - Provide analyses and support for effectiveness assessment. - Provide input for targeting effectiveness assessments for leadership acceptance. - Provide operations and reengagement recommendations. - Provide target recommendations which meet leadership objectives. - Provide targeting products and targeting support as designated. - Provide time sensitive targeting support.	

	- Review appropriate information sources to determine validity and relevance of information gathered. Sanitize and minimize information to protect sources and methods. - Support identification and documentation of collateral effects. - Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence - requirements are accurate and up-to-date.	
Target Network Analyst	- Provide expertise to course of action development. - Classify documents in accordance with classification guidelines. - Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas. - Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets. - Identify and conduct analysis of target communications to identify information essential to support operations. - Conduct nodal analysis. - Conduct quality control to determine validity and relevance of information gathered about networks. - Conduct target research and analysis. - Determine what technologies are used by a given target. - Apply analytic techniques to gain more target information. - 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.) - Generate requests for information. - Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. - Identify collection gaps and potential collection strategies against targets. - Identify network components and their functionality to enable analysis and target development. - Make recommendations to guide collection in support of customer requirements. - Provide subject matter expertise to development of exercises. - Perform content and/or metadata analysis to meet organization objectives. - Profile targets and their activities.	Absent

	- Provide target recommendations which meet leadership objectives. - Review appropriate information sources to determine validity and relevance of information gathered. - 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.	
Multi-Disciplined Language Analyst	- Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets. - Determine what technologies are used by a given target. - Identify collection gaps and potential collection strategies against targets. - Make recommendations to guide collection in support of customer requirements. - Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. - Advise managers and operators on language and cultural issues that impact organization objectives. - Analyze and process information using language and/or cultural expertise. - Assess, document, and apply a target's motivation and/or frame of reference to facilitate analysis, targeting and collection opportunities. - Collaborate across internal and/or external organizational lines to enhance collection, analysis and dissemination. - Conduct all-source target research to include the use of open source materials in the target language. - Conduct analysis of target communications to identify essential information in support of organization objectives. - Perform quality review and provide feedback on transcribed or translated materials. - Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing. - Identify cyber threat tactics and methodologies. - Identify target communications within the global network. - Maintain awareness of target communication tools, techniques, and the characteristics of target communication networks (e.g., capacity, functionality,	Absent

	paths, critical nodes) and their potential implications for targeting, collection, and analysis. - Provide feedback to collection managers to enhance future collection and analysis. - Perform foreign language and dialect identification in initial source data. - Perform or support technical network analysis and mapping. - Provide requirements and feedback to optimize the development of language processing tools. - Perform social network analysis and document as appropriate. - Scan, identify and prioritize target graphic (including machine-to-machine communications) and/or voice language material. - Tip critical or time-sensitive information to appropriate customers. - Transcribe target voice materials in the target language. - Translate (e.g., verbatim, gist, and/or summaries) target graphic material. - Translate (e.g., verbatim, gist, and/or summaries) target voice material. - Identify foreign language terminology within computer programs (e.g., comments, variable names). - Provide near-real time language analysis support (e.g., live operations). - Identify cyber/technology-related terminology in the target language.	
Cyber Intel Planner	- Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives. - Coordinate for intelligence support to operational planning activities. - Assess all-source intelligence and recommend targets to support cyber operation objectives. - Assess target vulnerabilities and/or operational capabilities to determine course of action. - Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives. - Assist in the development and refinement of priority information requirements. - Enable synchronization of intelligence support plans across partner organizations as required. - Provide input to the identification of cyber-related success criteria.	Absent

	- Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials). - Contribute to crisis action planning for cyber operations. - Contribute to the development of the organization's decision support tools if necessary. - Incorporate intelligence equities into the overall design of cyber operations plans. - Coordinate with intelligence planners to ensure that collection managers receive information requirements. - Coordinate with the intelligence planning team to assess capability to satisfy assigned intelligence tasks. - Coordinate, produce, and track intelligence requirements. - Coordinate synchronize and draft applicable intelligence sections of cyber operations plans. - Use intelligence estimates to counter potential target actions. - Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives. - Develop and review intelligence guidance for integration into supporting cyber operations planning and execution. - Develop detailed intelligence support to cyber operations requirements. - Develop potential courses of action. - Develop, implement, and recommend changes to appropriate planning procedures and policies. - Draft cyber intelligence collection and production requirements. - Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines. - Evaluate intelligence estimates to support the planning cycle. - Evaluate the conditions that affect employment of available cyber intelligence capabilities. - Incorporate intelligence and counterintelligence to support plan development. - Identify all available partner intelligence capabilities and limitations supporting cyber operations. - Identify, draft, evaluate, and prioritize relevant intelligence or information requirements.	

	- Identify cyber intelligence gaps and shortfalls for cyber operational planning. - Identify the need, scope, and timeframe for applicable intelligence environment preparation derived production. - Provide input to or develop courses of action based on threat factors. - Interpret environment preparations assessments to determine a course of action. - Issue requests for information. - Lead and coordinate intelligence support to operational planning. - Maintain relationships with internal and external partners involved in cyber planning or related areas. - Maintain situational awareness to determine if changes to the operating environment require review of the plan. - Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary. - Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. - Prepare for and provide subject matter expertise to exercises. - Provide cyber focused guidance and advice on intelligence support plan inputs. - Recommend refinement, adaption, termination, and execution of operational plans as appropriate. - Review and comprehend organizational leadership objectives and guidance for planning. - Scope the cyber intelligence planning effort. - Document lessons learned that convey the results of events and/or exercises.	
Cyber Ops Planner	- Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives. - Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement. - Assess target vulnerabilities and/or operational capabilities to determine course of action. - Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives. - Provide input to the identification of cyber-related success criteria. - Develop, review and implement all levels of planning guidance in support of cyber operations.	Absent

	- Contribute to crisis action planning for cyber operations. - Contribute to the development of the organization's decision support tools if necessary. - Coordinate with intelligence and cyber defense partners to obtain relevant essential information. - Use intelligence estimates to counter potential target actions. - Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives. - Develop and maintain deliberate and/or crisis plans. - Develop and review specific cyber operations guidance for integration into broader planning activities. - Develop cyber operations plans and guidance to ensure that execution and resource allocation decisions align with organization objectives. - Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations. - Develop potential courses of action. - Develop, implement, and recommend changes to appropriate planning procedures and policies. - Devise, document, and validate cyber operation strategy and planning documents. - Ensure operational planning efforts are effectively transitioned to current operations. - Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines. - Evaluate intelligence estimates to support the planning cycle. - Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives. - Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities. - Incorporate cyber operations and communications security support plans into organization objectives. - Identify cyber intelligence gaps and shortfalls for cyber operational planning. - Integrate cyber planning/targeting efforts with other organizations. - Interpret environment preparations assessments to determine a course of action.	

	- Issue requests for information. - Maintain relationships with internal and external partners involved in cyber planning or related areas. - Maintain situational awareness of cyber-related intelligence requirements and associated tasking. - Maintain situational awareness of partner capabilities and activities. - Maintain situational awareness to determine if changes to the operating environment require review of the plan. - Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives. - Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. - Provide subject matter expertise to planning efforts with internal and external cyber operations partners. - Prepare for and provide subject matter expertise to exercises. - Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs. - Provide input to the administrative and logistical elements of an operational support plan. - Provide planning support between internal and external partners. - Recommend refinement, adaption, termination, and execution of operational plans as appropriate. - Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities. - Submit or respond to requests for deconfliction of cyber operations. - Document lessons learned that convey the results of events and/or exercises.	
Partner Integration Planner	- Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement. - Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives. - Provide expertise to course of action development. - Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials).	Absent

	- Contribute to crisis action planning for cyber operations. - 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. - Coordinate with intelligence and cyber defense partners to obtain relevant essential information. - Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations. - Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives. - Develop strategy and processes for partner planning, operations, and capability development. - Develop, implement, and recommend changes to appropriate planning procedures and policies. - Develop, maintain, and assess cyber cooperation security agreements with external partners. - Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives. - Facilitate the sharing of "best practices" and "lessons learned" throughout the cyber operations community. - Identify and manage security cooperation priorities with external partners. - Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities. - Integrate cyber planning/targeting efforts with other organizations. - Maintain relationships with internal and external partners involved in cyber planning or related areas. - Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives. - Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy. - Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary. - Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. - Provide subject matter expertise to planning efforts with internal and external cyber operations partners.	

	- Propose policy which governs interactions with external coordination groups. - Prepare for and provide subject matter expertise to exercises. - Provide cyber focused guidance and advice on intelligence support plan inputs. - Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs. - Provide planning support between internal and external partners. - 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. - Serve as a liaison with external partners. - Submit or respond to requests for deconfliction of cyber operations. - Synchronize cyber international engagement activities and associated resource requirements as appropriate. - Synchronize cyber portions of security cooperation plans. - Document lessons learned that convey the results of events and/or exercises.	
Cyber Operator	- Analyze internal operational architecture, tools, and procedures for ways to improve performance. - Analyze target operational architecture for ways to gain access. - Collaborate with development organizations to create and deploy the tools needed to achieve objectives. - 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 on-net activities to control and exfiltrate data from deployed technologies. - Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies. - Conduct open source data collection via various online tools. - Conduct survey of computer and digital networks. - Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers).	Absent

	- Detect exploits against targeted networks and hosts and react accordingly. - Develop new techniques for gaining and keeping access to target systems. - Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems. - 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. - Maintain situational awareness and functionality of organic operational infrastructure. - Operate and maintain automated systems for gaining and maintaining access to target systems. - Conduct cyber activities to degrade/remove information resident in computers and computer networks. - Process exfiltrated data for analysis and/or dissemination to customers. - Provide real-time actionable geolocation information. - Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects. - Test and evaluate locally developed tools for operational use. - Test internal developed tools and techniques against target tools.	
Cyber Crime Investigator	- Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects. - Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet. - 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). - Examine recovered data for information of relevance to the issue at hand. - Fuse computer network attack analyses with criminal and counterintelligence investigations and operations. - Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.	Absent

	- Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations. - Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. - Identify elements of proof of the crime. - Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber - intrusion incidents, investigations, and operations. - Process crime scenes. - Secure the electronic device or information source. - Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence. - Analyze the crisis to ensure public, personal, and resource protection. - Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation. - Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks. - Provide criminal investigative support to trial counsel during the judicial process. - Analyze computer-generated threats for counter intelligence or criminal activity. - Gather and preserve evidence used on the prosecution of computer crimes. - 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. - Determine and develop leads and identify sources of information to identify and/or prosecute the responsible patties to an intrusion or other crimes. - Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking). - Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property. - Prepare reports to document the investigation following legal standards and requirements.	
Law Enforcement /Counter Intelligence Forensics Analyst	- Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet. - Establish relationships, if applicable, between the incident response team and other groups, both	Absent

	internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals). - Resolve conflicts in laws, regulations, policies, standards, or procedures. - Analyze incident data for emerging trends. - Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis. - Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances. - Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission. - 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). - Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities. - Analyze organizational cyber policy.	
Cyber Defense Forensics Analyst	- Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion. - Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis. - 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. - Decrypt seized data using technical means. - Provide technical summary of findings in accordance with established reporting procedures. - Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence. - Examine recovered data for information of relevance to the issue at hand.	Absent

	- Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. - 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. - Perform file signature analysis. - Perform hash comparison against established database. - Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView). - Perform timeline analysis. - 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). - Perform static media analysis. - Perform tier 1, 2, and 3 malware analysis. - Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures). - Provide technical assistance on digital evidence matters to appropriate personnel. - Recognize and accurately report forensic artifacts indicative of a particular operating system. - Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost). - Capture and analyze network traffic associated with malicious activities using network monitoring tools. - Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence. - Conduct cursory binary analysis. - Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. - Perform virus scanning on digital media. - Perform file system forensic analysis. - Perform static analysis to mount an "image" of a drive (without necessarily having the original drive). - Perform static malware analysis. - Utilize deployable forensics toolkit to support operations as necessary. - Coordinate with intelligence analysts to correlate threat assessment data. - Process image with appropriate tools depending on analyst's goals.	

	- Perform Windows registry analysis. - Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis. - Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired. - Correlate incident data and perform cyber defense reporting. - Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission. - 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. - Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information. - Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.	

7. **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**

- Due to the absence of secure software assessor, basic coding flaws can go undetected and can be exploited by malicious users for conducting various attacks.
- As systems security analyst is not present at our company, disaster recovery, business and continuity of operation plans may not be carried out properly.
- As cyber legal advisor is absent, legal analysis and proper guidance on laws, regulations, policies may not be overseen.
- Proper cyber training and education may not be received due to the absence of cyber instructor.
- As threat/warning analyst is absent, intelligence regarding threat activities, indications or warnings cannot be gathered in a timely manner.

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

- The service-oriented security architecture principles cannot be applied due to the absence of systems security analyst resulting in a loss of confidentiality, integrity, and availability requirements.
- Due to the absence of cyber legal advisor, any compliance risk may be a potential for financial losses and heavy fines.
- In the absence of cyber defense forensic analyst, any malicious attempts may go undetected
- Unauthorized access is a possibility by exploiting any coding vulnerabilities in the absence of a secure software assessor.
- Any events of data breach may lead to loss of reputation and trust.

9. **List of recommended policies (Hiring new Cybersecurity staff, Educating current staff, Outsourcing) for each recommended Cybersecurity Specialty Area, Cybersecurity Work Role, or Cybersecurity Task that should be created to mitigate the identified risks (it is not required to write detailed policies)**

- Software security assessor should be hired for analyzing the security of new applications or software code.
- A cyber legal advisor should be hired for providing advices and recommendations to the staff and upper management.
- A cyber instructor should be employed, and a curriculum should be developed for cyber training, education and awareness.
- In the threat analysis domain, both threat analyst and exploitation analyst should be hired for gathering intel on the cyber threats and for performing penetration testing operations.
- A cyber defense forensic analyst should be employed for analyzing and mitigation of network vulnerabilities.

Part C: Security Risk Management Recommendations (based on recommendations from Class Assignments 1-11) – this is the focus of the executive Class Presentation

C1. Security Risk Management Recommendations: Provide the list of recommended Prevention and Response controls, methods and policies based on your risk management analysis in Parts A and B above

For HGA:

- Physical controls are only partially implemented. Stricter physical access controls like RFID doors and fob controlled gates should be implemented in HGA.
- A more comprehensive contingency plan should be placed by COG to handle physical plant failures, natural disasters or for any other major equipment malfunctions.
- Stricter user control and media access policies like no USB policy should be implemented.
- Stronger Identification and authentication policies like 2 factor authentications should be implemented.
- Data integrity tools and checks like parity check and cyclic redundancy checks should be implemented for ensuring data integrity for time and attendance data.
- Auditing logging capabilities should be implemented to detect any malicious attempts.
- Data should be encrypted at all times which included at rest, in-transit and also in-memory.
- Controls Mitigating Vulnerabilities Related to Payroll Fraud
- Controls Mitigating Payroll Error
- Controls Mitigating Vulnerabilities Related to Continuity of Operations
- Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of information
- Controls Vulnerabilities Related to Network-Related Attacks

For my company:

Access Control Security Risk Management Implementation Controls and Policies

- Biometric systems need to be implemented for improved authentication. They provide improved security and also cannot be forgotten or lost.
- Implementing a deny by default policy on the company firewall provides us with a better control over authorization. All the ingress traffic from the internet is denied by default.
- Logical Network Port Security should be implemented so that all the unnecessary ports can be closed and be less susceptible to attacks from the internet.

- Data loss prevention software should be implemented to protect all the sensitive information and to tighten endpoint security
- Data Activity Monitoring (DAM) solution can be implemented to closely monitor traffic and to avoid data leaks. An average hacker conducts reconnaissance six months before the actual breach, hence monitoring for unusual behavior can help deter a data breach.
- A Host based Intrusion Detection System and Network based Intrusion Detection System can be implemented for closely monitoring, analyzing the packets, logging and notifying authorities.
- Full scans must be run for malware from time to time basis.

Network Infrastructure Security Risk Management Implementation Controls and Policies

- Network TAPs needs to be implemented to monitor and detect malicious activities by analyzing quality packet captures.
- Wireless IDS need to be implemented to detect WLAN attacks and DOS attacks
- Implementation of deep packet inspection and hybrid firewall technologies is crucial as they can be able to detect malicious payload and prevent some critical cyber-attacks on the organization.
- Network TAPs and Data Activity Monitoring (DAM) solution can be implemented to closely monitor traffic and to avoid data leaks. An average hacker conducts reconnaissance six months before the actual breach, hence monitoring for unusual behavior can help deter a data breach.
- A Wireless Intrusion Detection System and Network based Intrusion Detection System can be implemented for closely monitoring, analyzing the packets, logging and notifying authorities.
- Full scans must be run for malware from time to time basis.
- Backdoors could be implemented by the organization for admins to regain control of the systems after the attacker has compromised and changed the credentials of the critical applications and services.

Network Infrastructure Management Security Risk Management Implementation Controls and Policies

- Out of Band management should be implemented alongside In band management as it is one of the best practices to manage network devices effectively.
- Signature-based, Anomaly-based or rule-based NIDS needs to be implemented to efficiently detect DOS attacks and other malware.

- Host-to-Host VPN should be implemented for a secure IPSec connection using RSA between the hosts for secure data transfers and communications.
- It good to hire DDOS mitigation services which can handle high amounts of traffic and have data scrubbing centers in case of DOS attacks.
- RSA key sizes should be increased to 4096 bits to safeguard against any possible attacks
- SNMP Management system can be implemented to better analyze and monitor performance.
- SNMPv2 should be stopped and SNMPv3 should be adopted completely as it uses much secure AES encryption standard.

Database Security Risk Management Implementation Controls and Policies

- Implementing Time and Count limits on Network session parameters can greatly increase the security of the database while prevent many malicious attack attempts.
- Boundary defense needs to be implemented which acts like a first line of defense to safeguard sensitive information and keep the malicious traffic out from the internal network.
- Warning messages can also be implemented to detect any malicious attempts.
- security support structure positioning should be implemented to ascertain the security policies are safeguarded from malicious users.
- It is good to implement clustering and federated databases to recover quickly against DOS attacks and reduce downtime.
- Following good configuration management practices, the visibility, performance and efficiency can be increased deterring data breaches and reducing the risk of outages.
- security support structure positioning should be implemented to ascertain the security policies are safeguarded from malicious users
- In the event of system failures and corruptions trusted recovery can help recover thus promoting business continuity.

Applications Development Security Risk Management Implementation Controls and Policies

- All the data in memory should be cleared after use and all the data should also be encrypted in memory when not in use.
- Data marking policies should be implemented to avoid risk of information disclosure.
- PKI certificates validation should be enforced properly for the ascertain the effectiveness of PKI certificates.
- Message authentication codes and hashes should be implemented to ensure data confidentiality, integrity and availability.

- Session limits should be implemented to avoid DOS and other attacks.
- Security controls like ACL's and permissions should be implemented for applications with excessive privileges.
- Automated tools should be implemented for testing which maximizes the chances of finding coding errors and other vulnerabilities.
- Combination of client server application authentication should be implemented to streamline the process of authentication.
- Classified Audit record content should be followed to classify and prioritize audit events.
- Use of open source catalog can be helpful in developing secure applications and testing policies should also be implemented by open source software.

Wireless Security Risk Management Implementation Controls and Policies

- Additional protocols like PEAP should be used to ensure data confidentiality and integrity.
- Authorized architecture should be implemented to secure the wireless access points and bridges.
- Secure Wireless networking and security boundary controls must be implemented for all projects, not just govt. projects.
- RSN can be implemented to prevent MAC address spoofing and other sniffing attacks.
- Wireless two-way email can be implemented for securing wireless emails for additional security.
- SSIDs can be made hidden which makes the attackers work harder to carry out a successful attack.
- Secure Mobile Environment PED can be used for secure voice and data communication.
- Bluetooth mice and keyboard should be replaced with wired counterparts.

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:

Total Cost of additional controls and policies = $1,531,000

Residual risk with current security controls = $30,056,000

Residual risk with current controls, new controls, missing MOT controls, VPN and DMZ (mixed strategy) = $12,384,089

Residual Risk Reduction = Residual risk with current controls – Residual risk with current controls, new controls, missing MOT controls, VPN and DMZ (mixed strategy)

= $30,056,000 - $12,384,089

= $17,671,911

Thus, residual risk reduction exceeds the budget for proposed controls.

Cost Benefit ratio = (proposed security risk budget cost) / (expected security risk benefit)

= $1,531,000 / $17,671,911

= 0.0866

For my company:

Total cost of recommended controls and policies = $35,000,000

Residual risk reduction = $82,000,000

Cost Benefit Ratio = $35,000,000/$82,000,000

= 0.4268

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.

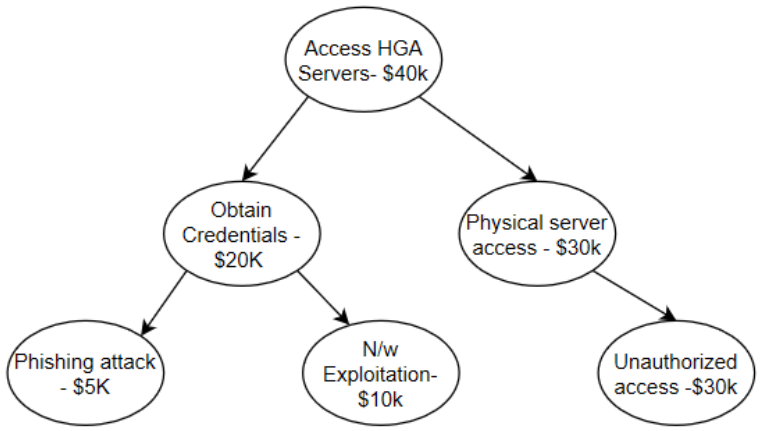
Point of Comparison	HGA	My Company
Industry	Government Payroll Agency	Healthcare Solutions Provider
Mission	Transferring U.S. Government funds to individuals in the form of paychecks	To provide comprehensive clinical documentation, along with solutions for Practice Management, Population Health, Patient Engagement, and Revenue Cycle Management
Critical Assets in $	$35,000,000	$300,000,000
Exploitation Probability	60%	35%
Asset Risks and Vulnerability Risks in $	Asset Risks = $12,500,000 Vulnerability Risks = $7,300,000	Asset Risks = $28,500,000 Vulnerability Risks = $12,400,000
Proposed IA security controls and budget :		
$ security policies and control budget	$1,531,000	$35,000,000

Cost Benefit Ratio	0.0866	0.4268
Geographical Presence	USA	USA
Number of employees	1000	5000
Threat Agents	Intelligence States, Insider Threats , Natural disasters, Hacker groups	Hacker groups, Natural disasters, Insider threats.

- **For HGA:**

Threat Environment:

- **Attack Tree Scenario:**



- **List of Security Vulnerabilities:**

No.	Vulnerabilities
T1:V1	Vulnerabilities related to payroll fraud
V1.1	Falsified Time Sheets
V1.2	Unauthorized Access
V1.3	Bogus Time and Attendance Applications
V1.4	Unauthorized Modifications of Time and Attendance Sheets
T2:V2	Vulnerabilities Related to Payroll Errors
T3:V3	Vulnerabilities Related to Continuity of Operations
V3.1	COG Contingency Planning
V3.2	Division Contingency Planning
V3.3	Virus Prevention
V3.4	Accidental Corruption and Loss of Data
T4:V4	Vulnerabilities Related to Disclosure or Brokerage of information
T5:V5	Vulnerabilities Related to Network-Related Attacks

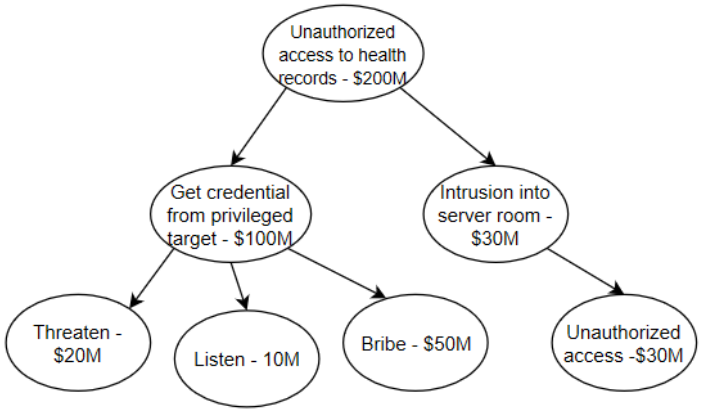
- **Cybersecurity Workforce Recommendations:**

  - Physical controls are only partially implemented. Stricter physical access controls like RFID doors and fob controlled gates should be implemented in HGA.
  - A more comprehensive contingency plan should be placed by COG to handle physical plant failures, natural disasters or for any other major equipment malfunctions.
  - Stricter user control and media access policies like no USB policy should be implemented.
  - Stronger Identification and authentication policies like 2 factor authentications should be implemented.
  - Data integrity tools and checks like parity check and cyclic redundancy checks should be implemented for ensuring data integrity for time and attendance data.
  - Auditing logging capabilities should be implemented to detect any malicious attempts.
  - Data should be encrypted at all times which included at rest, in-transit and also in-memory.
  - Controls Mitigating Vulnerabilities Related to Payroll Fraud
  - Controls Mitigating Payroll Error
  - Controls Mitigating Vulnerabilities Related to Continuity of Operations
  - Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of information
  - Controls Vulnerabilities Related to Network-Related Attacks

➢ **For my Company:**

Threat Environment:

- **Attack Tree Scenario:**



Vulnerabilities:

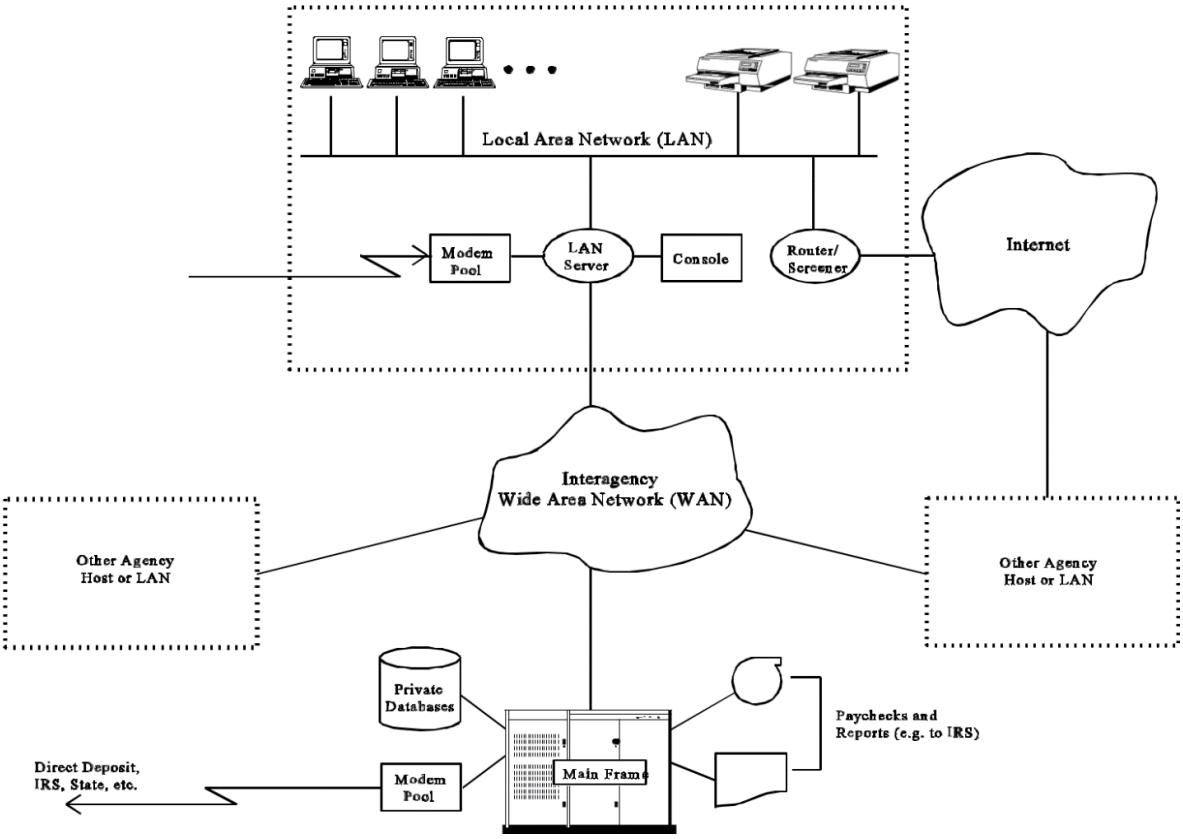
6. Disclosure of sensitive information
7. Unauthorized access: Due to the absence of network TAPs, data cannot be properly monitored and collected. This can lead to unauthorized access not being detected.
8. Disclosure of sensitive information: Attacks like eavesdropping can play a role in disclosure of information.
9. Denial of Service: DOS attacks are a possibility due to the absence of boundary defenses and recovery can be difficult due to missing controls like clustering and federation. This can have a high impact to our organization as providing services to 850,000+ healthcare professionals are paramount.
10. Data Integrity and Authenticity can be compromised as message authentication codes and hashes are not used. Data confidentiality can be compromised as data in memory can be accessed by a malicious user.

Cybersecurity Workforce Recommendations:

- Software security assessor should be hired for analyzing the security of new applications or software code.
- A cyber legal advisor should be hired for providing advices and recommendations to the staff and upper management.
- A cyber instructor should be employed, and a curriculum should be developed for cyber training, education and awareness.
- In the threat analysis domain, both threat analyst and exploitation analyst should be hired for gathering intel on the cyber threats and for performing penetration testing operations.
- A cyber defense forensic analyst should be employed for analyzing and mitigation of network vulnerabilities.

Part D:

Appendix 3: Detailed Network Topology for HGA



Appendix 4: Detailed Network Topology (defense-in-depth) for your company