RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SBX1-R07

Top 10 ICS Cybersecurity Problems Observed in Critical Infrastructure

Bryan Hatton

Cyber Security Researcher
Idaho National Laboratory
In support of DHS ICS-CERT
@phaktor

#RSAC

16 Critical Infrastructure Sectors

Presidential Policy Directive 21 (PPD-21) categorized U.S. critical infrastructure into the following 16 CI sectors.

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food & Agriculture
- Government Facilities
- Healthcare & Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

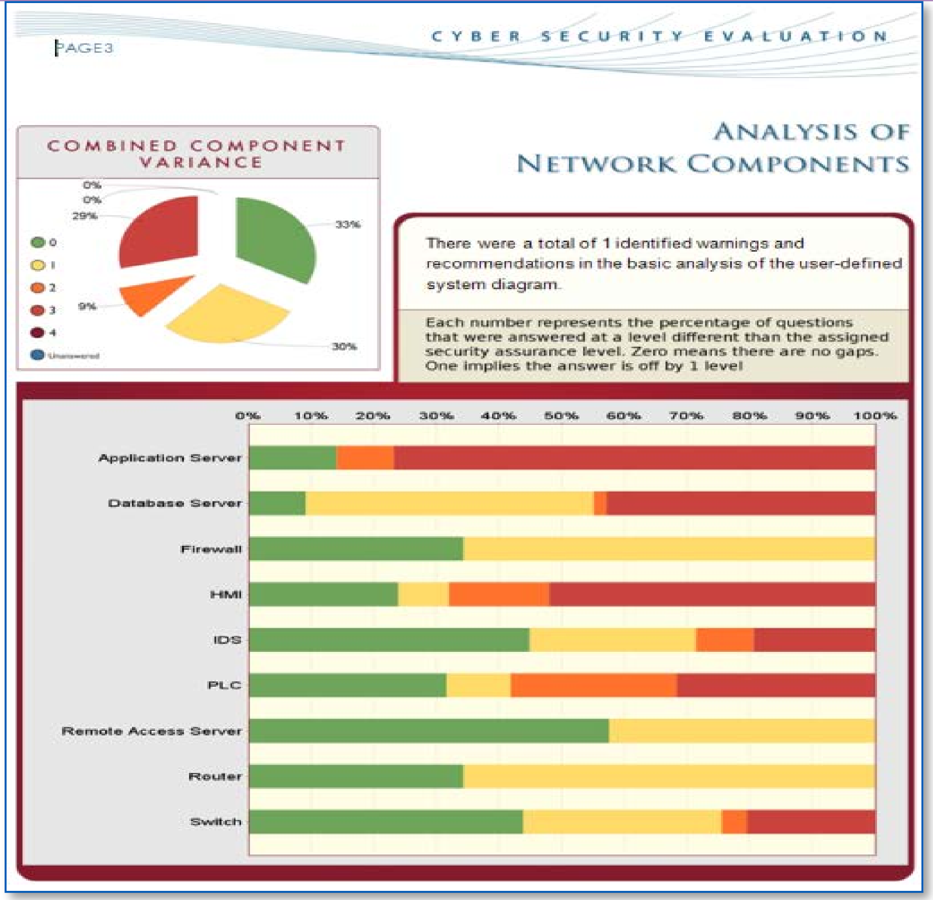
Many of the processes controlled by computerized control systems have advanced to the point that they can no longer be operated without the control system

Homeland Security

Data Set - 20 Sources

Critical Manufacturing	1
Dams	1
Energy	6
Government Facilities	2
Water Plants	10

CSET®

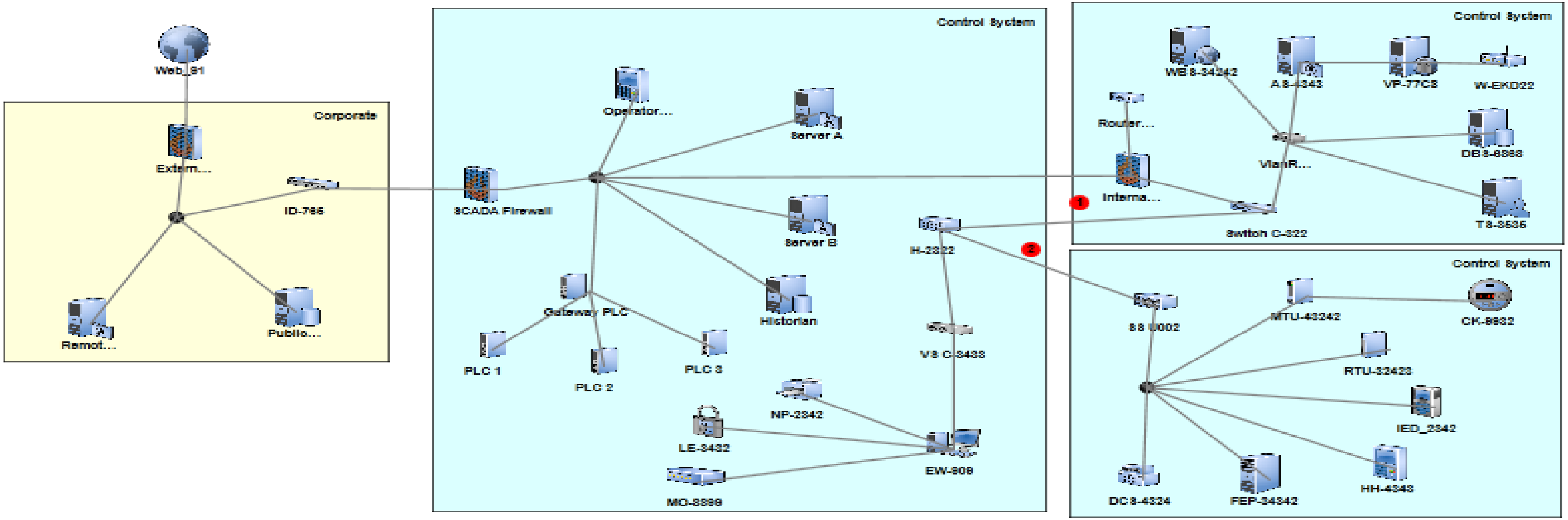


ANALYSIS OF NETWORK COMPONENTS

There were a total of 1 identified warnings and recommendations in the basic analysis of the user-defined system diagram.

Each number represents the percentage of questions that were answered at a level different than the assigned security assurance level. Zero means there are no gaps. One implies the answer is off by 1 level

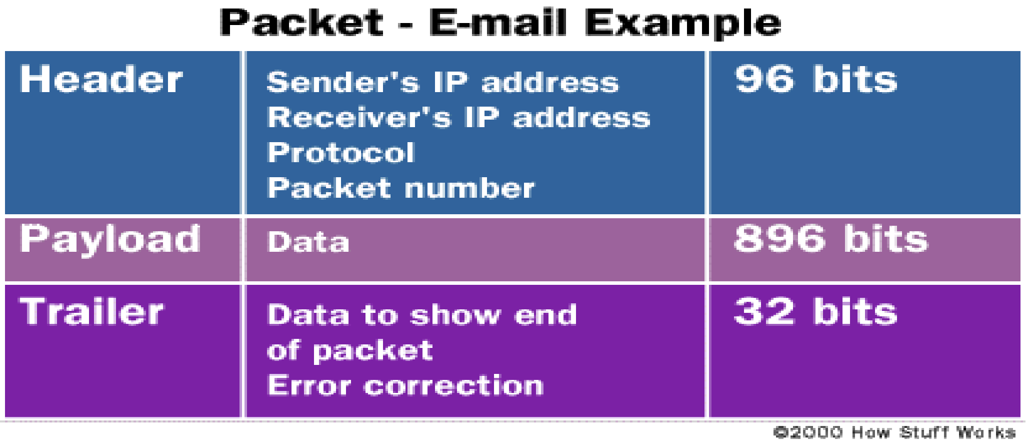
Design Architecture Reviews



Network Architecture Verification & Validation

NAVV Benefits:

- TCP Header Data Network Capture
- Point-to-Point Communication Verifications
- Data Flow Validation
- Network Perimeter Protection



Packet - E-mail Example

Header	Sender's IP address Receiver's IP address Protocol Packet number	96 bits
Payload	Data	896 bits
Trailer	Data to show end of packet Error correction	32 bits

©2000 How Stuff Works

10. AC-6 Least Privilege

Mitigations

- Establish user accounts for Administrators
- Appropriate use of the escalate privilege function
- Review work requirements for necessary access requirements

9. CM-3 Configuration Change Control

Mitigations

- Establish a solid configuration change control process
- Keep records / Use an automated software
- Have staff that “know” your ICS
- Keep patches for devices and applications current

8. PE-3 Physical Access Control

Mitigations

- Access Alarms
- Video Surveillance
- Electronic Keys / RFID

7. AU-12 Audit Generation

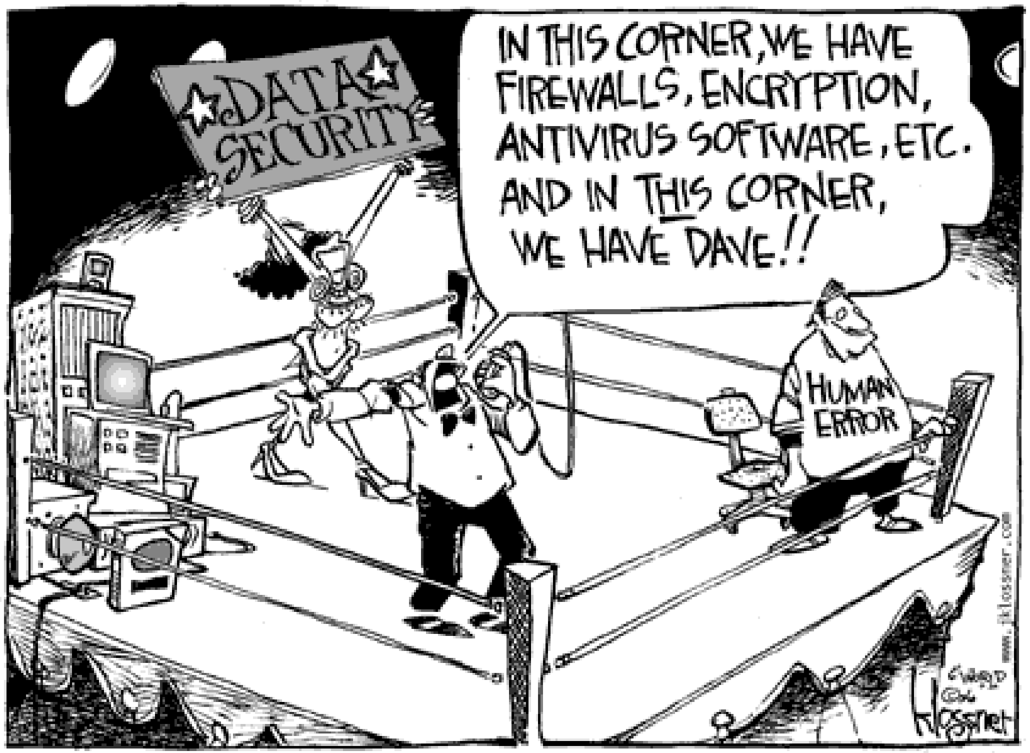
Mitigations

- Establish a process to collect logs
- Develop of system of processing logs to find “events of interest”
- Collect logs in a centralized location outside of data source

6. AT-2 Security Awareness Training

Mitigations

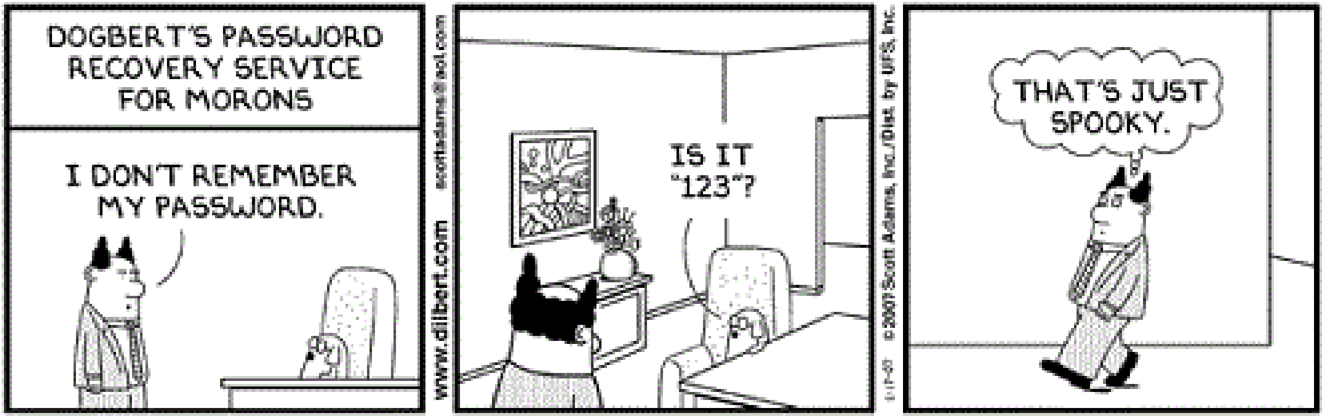
- Establish annual training program to bring workers up to speed.


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

5. IA-5 Authenticator Management

Mitigations

- Good Password Policies and Processes
- Use Account Management Software to enforc policy


DOGBERT'S PASSWORD RECOVERY SERVICE FOR MORONS
I DON'T REMEMBER MY PASSWORD.
scottadams@aol.com
www.dilbert.com
IS IT "123"?
©2001 Scott Adams, Inc./Dist. by UFS, Inc.
THAT'S JUST SPOOKY.

© Scott Adams, Inc./Dist. by UFS, Inc.

4. SA-2 Allocation of Resources

Mitigations

- Asset owners need more dedicated staff
- Staff on location

3. CM-7 Least Functionality

Mitigations

- Determine needed services and deny all others
- Apply hardening as applicable
- Use whitelisting

"Do you really think it was necessary to whitelist Megan Fox on your android?

2. IA-2 Identification and Authentication

Mitigations

- Use good encryption for storage and transmission of credentials
- Uniquely identify personnel were possible
- Use multi-factor authentication for remote access and critical administrative access

1. SC-7 Boundary Protection

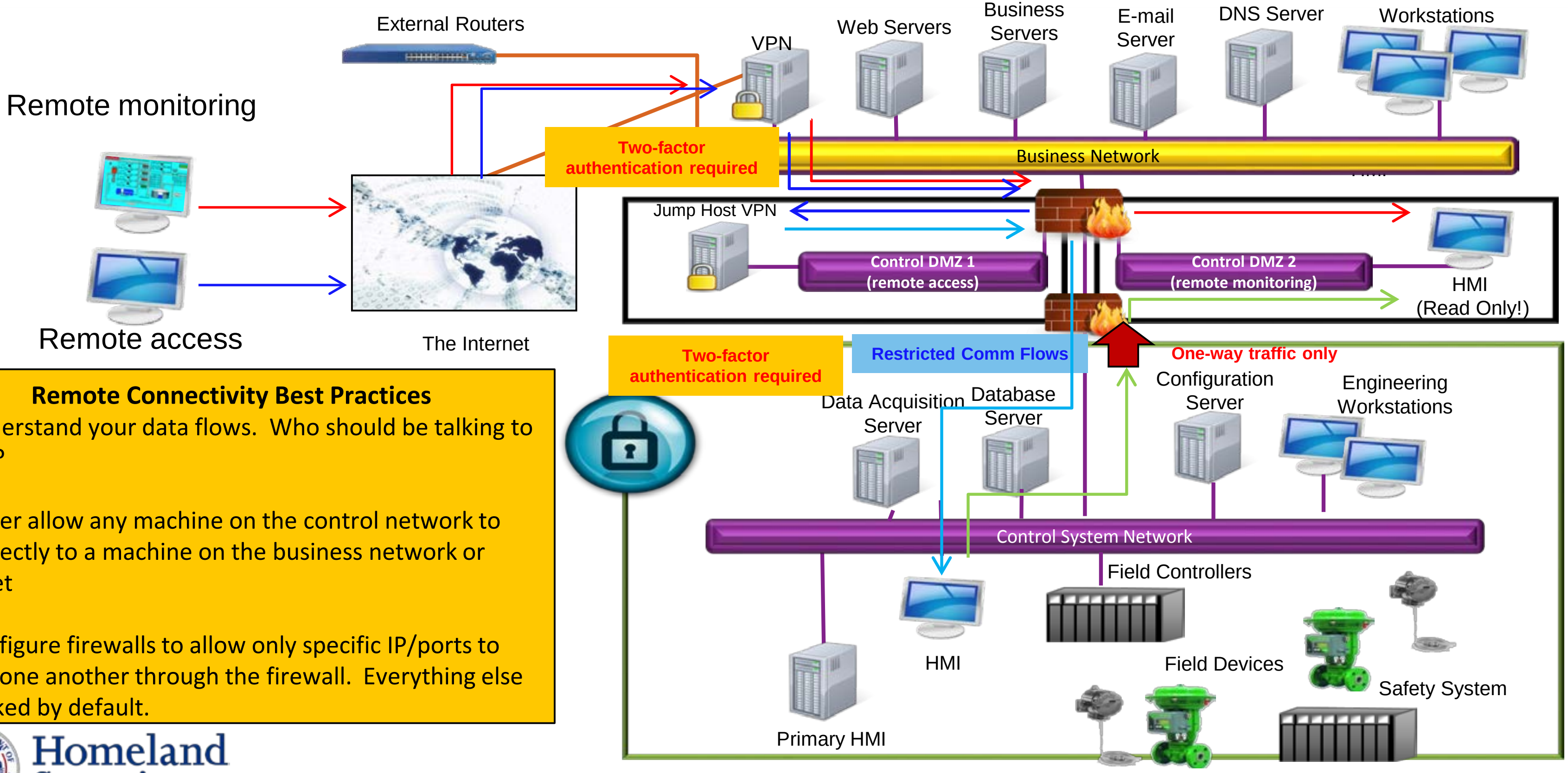
Mitigations

- Logically segment networks
- Establish strong firewall rules to route traffic
- Isolate security and support functions
- Deny traffic by default

Remote Access

- Use access points/jump servers for remote access
- Prevent split tunneling

Remote Access / Monitoring



Remote Connectivity Best Practices

1. Understand your data flows. Who should be talking to whom?

2. Never allow any machine on the control network to talk directly to a machine on the business network or Internet

3. Configure firewalls to allow only specific IP/ports to talk to one another through the firewall. Everything else is blocked by default.

Homeland Security

Observed Vulnerabilities – Top 11

1	SC-7 Boundary Protection	16.22%
2	IA-2 Identification and Authentication (Organizational Users)	7.34%
3	CM-7 Least Functionality	6.56%
4	SA-2 Allocation of Resources	4.63%
5	IA-5 Authenticator Management	4.25%
6	AT-2 Security Awareness Training	4.25%
7	AU-12 Audit Generation	4.25%
8	PE-3 Physical Access Control	4.25%
9	CM-3 Configuration Change Control	4.25%
10	AC-6 Least Privilege	4.25%
11	CP-9 Information System Backup	4.25%
		64.48%

Top 11 by Sector

	Energy	Gov Fac	Water	Total
SC-7 Boundary Protection	32.50%	25.00%	20.88%	25.15%
IA-2 Identification and Authentication (Organizational Users)	12.50%	10.00%	10.99%	11.38%
CM-7 Least Functionality	15.00%	10.00%	8.79%	10.18%
SA-2 Allocation of Resources	10.00%	5.00%	5.49%	7.19%
IA-5 Authenticator Management	2.50%	15.00%	6.59%	6.59%
CM-3 Configuration Change Control	10.00%	10.00%	4.40%	6.59%
AT-2 Security Awareness Training	2.50%	5.00%	8.79%	6.59%
PE-3 Physical Access Control	0.00%	15.00%	7.69%	6.59%
AC-6 Least Privilege	7.50%	0.00%	6.59%	6.59%
AU-12 Audit Generation	5.00%	5.00%	8.79%	6.59%
CP-9 Information System Backup	2.50%	0.00%	10.99%	6.59%
Grand Total	**100.00%**	**100.00%**	**100.00%**	**100.00%**

Operation Controls

CM-7 Least Functionality	14.29%
CP-9 Information System Backup	9.24%
PE-3 Physical Access Control	9.24%
AT-2 Security Awareness Training	9.24%
CM-3 Configuration Change Control	9.24%
CM-2 Baseline Configuration	7.56%
AT-3 Role-Based Security Training	7.56%
SI-4 Information System Monitoring	7.56%
CM-6 Configuration Settings	7.56%
MA-2 Controlled Maintenance	6.72%
MP-7 Media Use	5.88%
CM-4 Security Impact Analysis	5.88%
Grand Total (12)	**100.00%**

Management Controls

SA-2 Allocation of Resources	25.00%
SA-3 System Development Life Cycle	18.75%
SA-4 Acquisition Process	8.33%
PL-2 System Security Plan	8.33%
RA-5 Vulnerability Scanning	6.25%
CA-5 Plan of Action and Milestones	6.25%
PL-1 Security Planning Policy and Procedures	6.25%
CA-2 Security Assessments	6.25%
CA-3 System Interconnections	4.17%
SA-11 Developer Security Testing and Evaluation	2.08%
SA-8 Security Engineering Principles	2.08%
SA-12 Supply Chain Protection	2.08%
CA-7 Continuous Monitoring	2.08%
RA-3 Risk Assessment	2.08%
Grand Total (14)	**100.00%**

Technical Controls

SC-7 Boundary Protection	28.97%
IA-2 Identification and Authentication (Organizational Users)	13.10%
IA-5 Authenticator Management	7.59%
AU-12 Audit Generation	7.59%
AC-6 Least Privilege	7.59%
AC-2 Account Management	6.90%
SC-8 Transmission Confidentiality and Integrity	5.52%
AC-17 Remote Access	4.83%
SC-28 Protection of Information at Rest	4.14%
AC-20 Use of External Information Systems	3.45%
AC-18 Wireless Access	3.45%
AC-4 Information Flow Enforcement	3.45%
AC-19 Access Control for Mobile Devices	3.45%
Grand Total (14)	100%

Questions

?

11. CP-9 Information System Backup

Examples

- No backup servers
- No testing of backups or backup media
- No offsite storage

Mitigations

- Determine what should be backed up
- Implement a backup solution
- Test backups
- Keep an offsite copy for disaster recovery

Observed Vulnerabilities – Top 12-22

12	AC-2 Account Management	3.86%
13	CM-2 Baseline Configuration	3.47%
14	SA-3 System Development Life Cycle	3.47%
15	SI-4 Information System Monitoring	3.47%
16	AT-3 Role-Based Security Training	3.47%
17	CM-6 Configuration Settings	3.47%
18	SC-8 Transmission Confidentiality and Integrity	3.09%
19	MA-2 Controlled Maintenance	3.09%
20	CM-4 Security Impact Analysis	2.70%
21	AC-17 Remote Access	2.70%
22	MP-7 Media Use	2.70%
		35.52%