

AN OFFERING IN THE BLUE CYBER SERIES:

Cost Effective Cybersecurity

Presented by

Dr. Paul Shaw

Professor, Defense Acquisition University

May 2022

#27 in the Blue Cyber Education Series



Cost Effective Cybersecurity



Dr. Paul Shaw
Professor, Cybersecurity
Defense Acquisition University (DAU)

Computer Network Vulnerabilities

SECURITY CONTROLS FOR COMPUTER SYSTEMS (U)

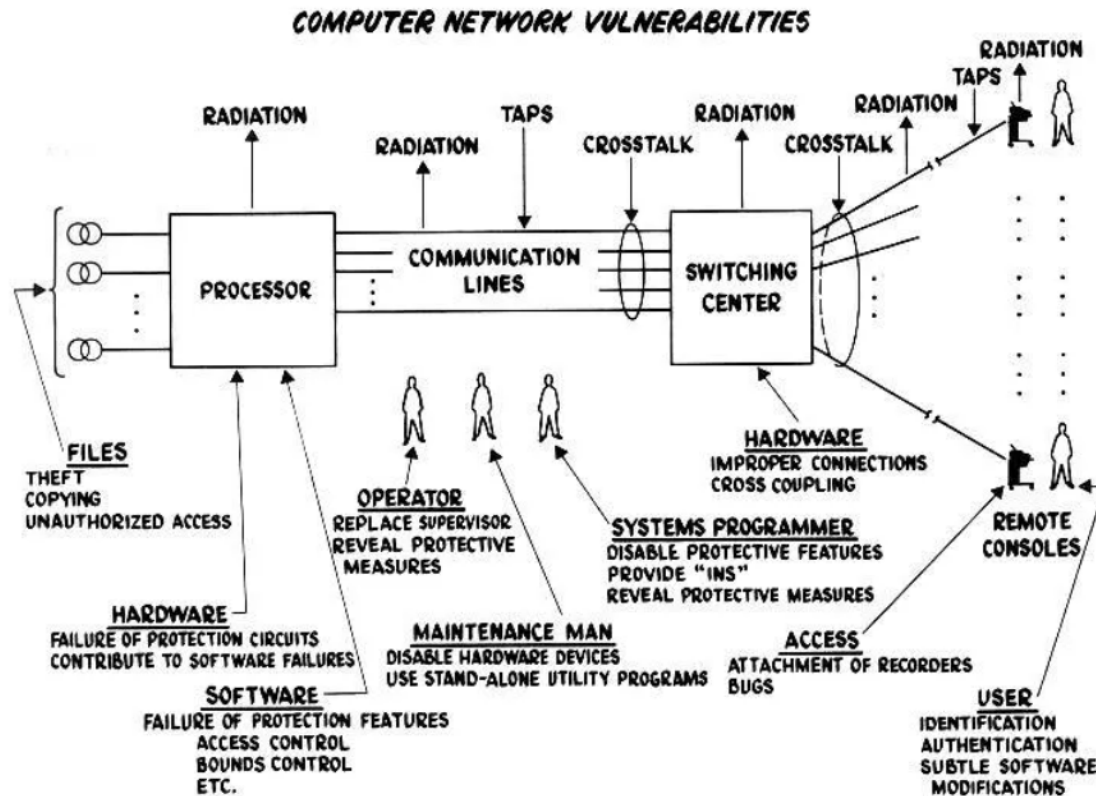
Report of Defense Science Board
Task Force on Computer Security



This diagram is from a DoD Study by Rand (also known as the Ware Report).

Does anyone know when this Report was published?

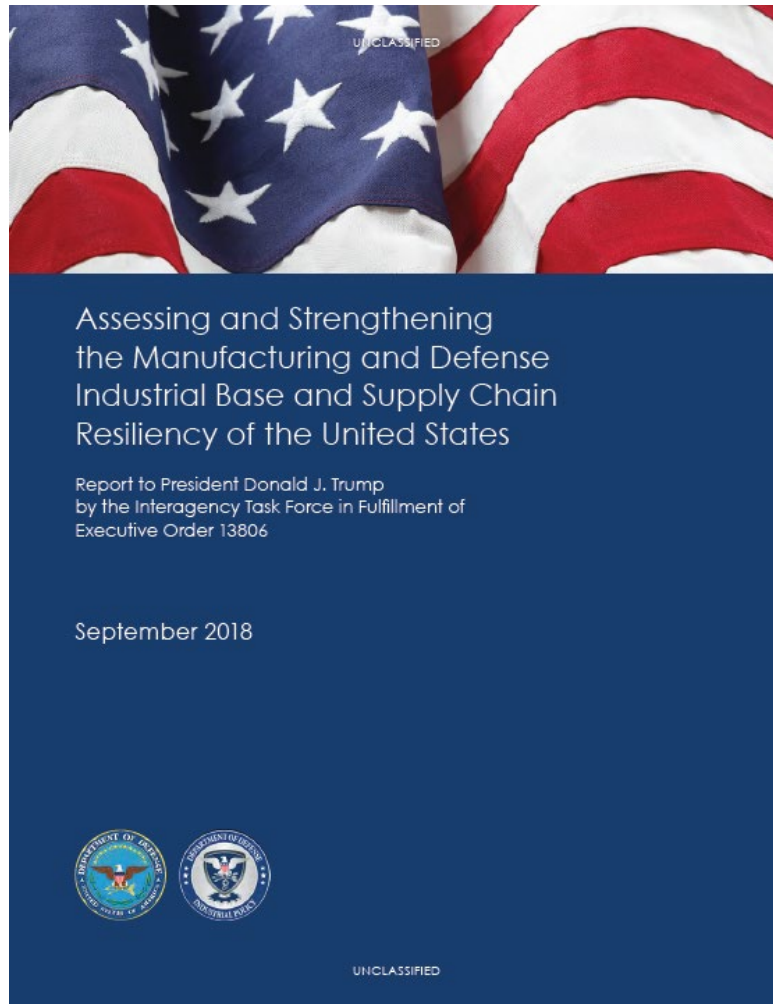
Defined threats are to the Data, Software, Hardware, Personnel Access, Transmission, Endpoints, and the Supply Chain



(p. 6)

<https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ware70.pdf>

State of Cybersecurity



“Of the approximately 347,000 manufacturers in the United States, 99% are small and medium-sized manufacturers, yet more than 50% lack basic cyber controls. An assessment by Bureau of Industry and Security illustrated the cybersecurity vulnerability of small manufacturers. The survey of over 9,000 “classified contract facilities” documented that 6,650 small facilities lagged medium and large firms across a broad range of 20 cybersecurity measures. It also found that fewer than half of the small firms had cybersecurity measures in place.” (p. 87 – 88)

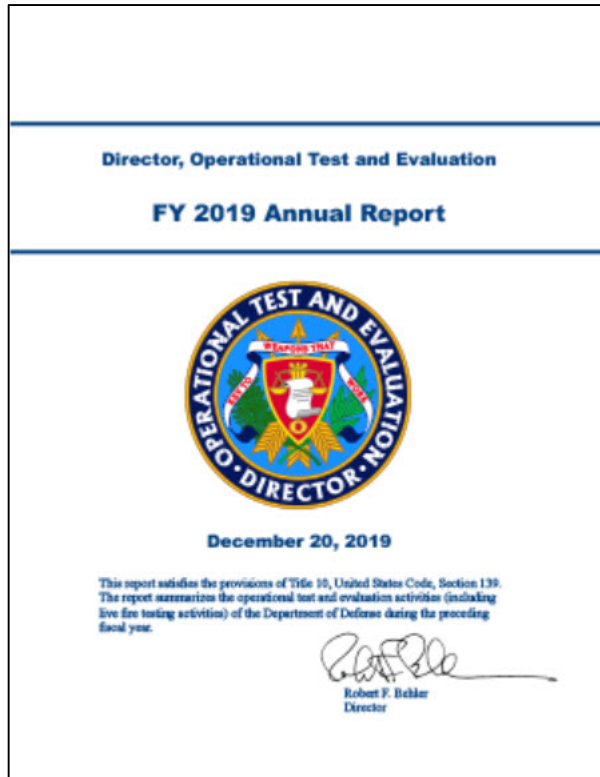
<https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF>

DoD T&E Annual Reports to Congress

Breaches of Contractors Give Advantage to Adversary.

“Breaches of cleared defense contractors provide adversaries with information that enables the development of cutting-edge weapons to be used against us, paves the way for cyber-attacks that could compromise critical DOD missions, and degrades our technical and commercial advantages.”

DOT&E analyzed past breaches of defense contractors for several major programs and found that these breaches exposed extensive information that empowers our adversaries to degrade key DoD systems and missions. DOT&E also observed several supply-chain table top exercises where significant efforts were being implemented to help shield critical design information and software from adversaries. Efforts such as these should be implemented for all critical programs, and operational assessments and monitoring of contractor networks, tools, facilities, and software factories should become routine for critical programs.” (DOT&E FY19 Annual Report, p. 230)



<https://www.dote.osd.mil/annualreport/>

Potential Impact

“The protection of unclassified federal information in nonfederal systems and organizations is dependent on the federal government providing a disciplined and structured process for identifying the different types of information that are routinely used by federal agencies.” NIST 171 r1, p. 1

The security requirements described in this publication have been developed based on three fundamental assumptions:

- Statutory and regulatory requirements for the protection of CUI are consistent, whether such information resides in federal systems or nonfederal systems including the environments in which those systems operate;
- Safeguards implemented to protect CUI are consistent in both federal and nonfederal systems and organizations; and
- The confidentiality impact value for CUI is no less than moderate in accordance with Federal Information Processing Standards (FIPS) Publication 199.


NIST 171 R 1, p. 5

Factor	Weight	Description
Network Security	Medium	Detecting insecure network settings
DNS Health	Medium	Detecting DNS insecure configurations and vulnerabilities
Patching Cadence	Medium	Out of date company assets which may contain vulnerabilities or risks
Endpoint Security	Medium	Measuring security level of employee workstations
IP Reputation	High	Detecting suspicious activity, such as malware or spam, within your company network
Application Security	Medium	Detecting common website application vulnerabilities
Cubit Score	Low	Proprietary algorithms checking for implementation of common security best practices
Hacker Chatter	Low	Monitoring hacker sites for chatter about your company
Information Leak	Medium	Potentially confidential company information which may have been inadvertently leaked
Social Engineering	Low	Measuring company awareness to a social engineering or phishing attacks

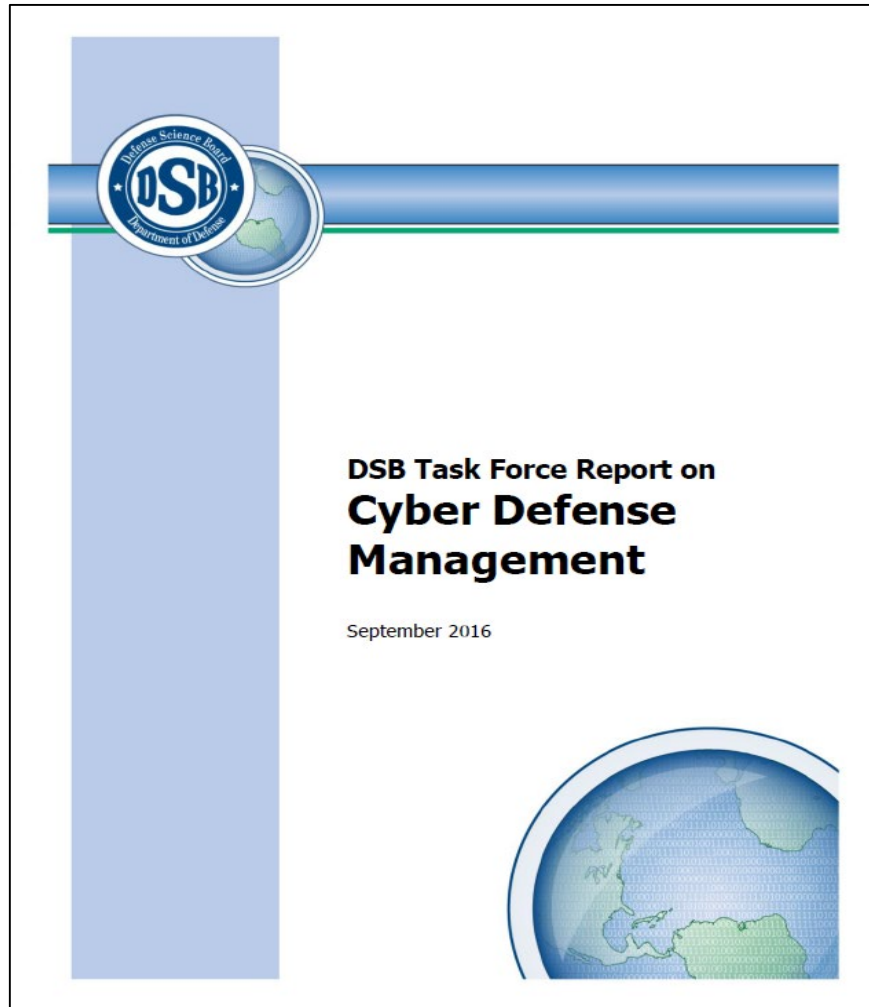
<https://securityscorecard.com/blog/securityscorecard-10-risk-factors-explained>

Potential Impact

“With regard to *federal information systems*, requirements in the federal regulation for protecting CUI at the moderate confidentiality impact level will be based on applicable policies established by OMB and applicable government wide standards and guidelines issued by NIST.” NIST 171 r1, p. v

	POTENTIAL IMPACT		
Security Objective	LOW	 MODERATE	HIGH
<i>Confidentiality</i> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Basic CYBER Investments



“One of the most important steps for improving the United States’ overall cybersecurity posture is for companies to prioritize the networks and data that they must protect and to invest in improving their own cybersecurity. While the U.S. government must prepare to defend the country against the most dangerous attacks, the majority of intrusions can be stopped through relatively basic cybersecurity investments that companies can and must make themselves.” (p. 5)

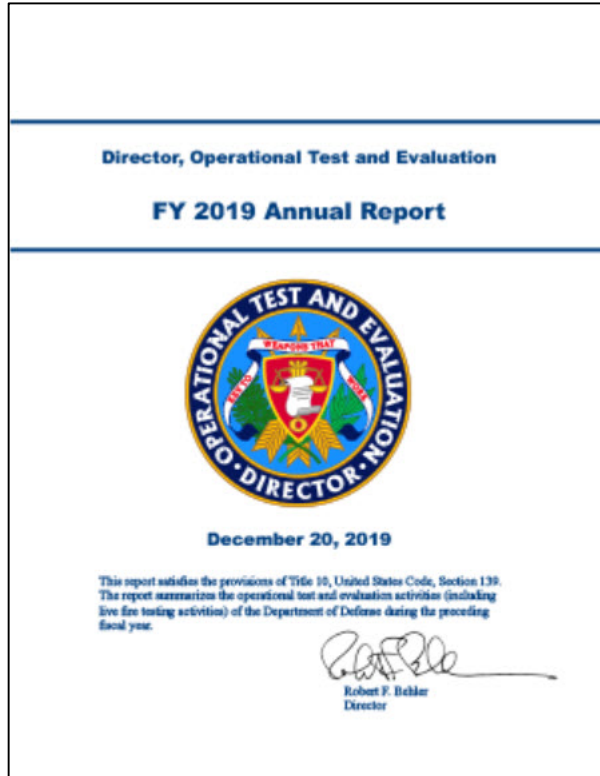
https://dsb.cto.mil/reports/2010s/Cyber_Defense_Management.pdf

DoD T&E Report

Breaches of Contractors Give Advantage to Adversary.

“Breaches of cleared defense contractors provide adversaries with information that enables the development of cutting-edge weapons to be used against us, paves the way for cyber-attacks that could compromise critical DOD missions, and degrades our technical and commercial advantages.”

DOT&E analyzed past breaches of defense contractors for several major programs and found that these breaches exposed extensive information that empowers our adversaries to degrade key DOD systems and missions. DOT&E also observed several supply-chain table top exercises where significant efforts were being implemented to help shield critical design information and software from adversaries. Efforts such as these should be implemented for all critical programs, and operational assessments and monitoring of contractor networks, tools, facilities, and software factories should become routine for critical programs.” (DOT&E FY19 Annual Report, p. 230)



<https://www.dote.osd.mil/annualreport/>

Your Environment

SANS

SANS Institute
Information Security Reading Room

**Effectively Addressing
Advanced Threats**

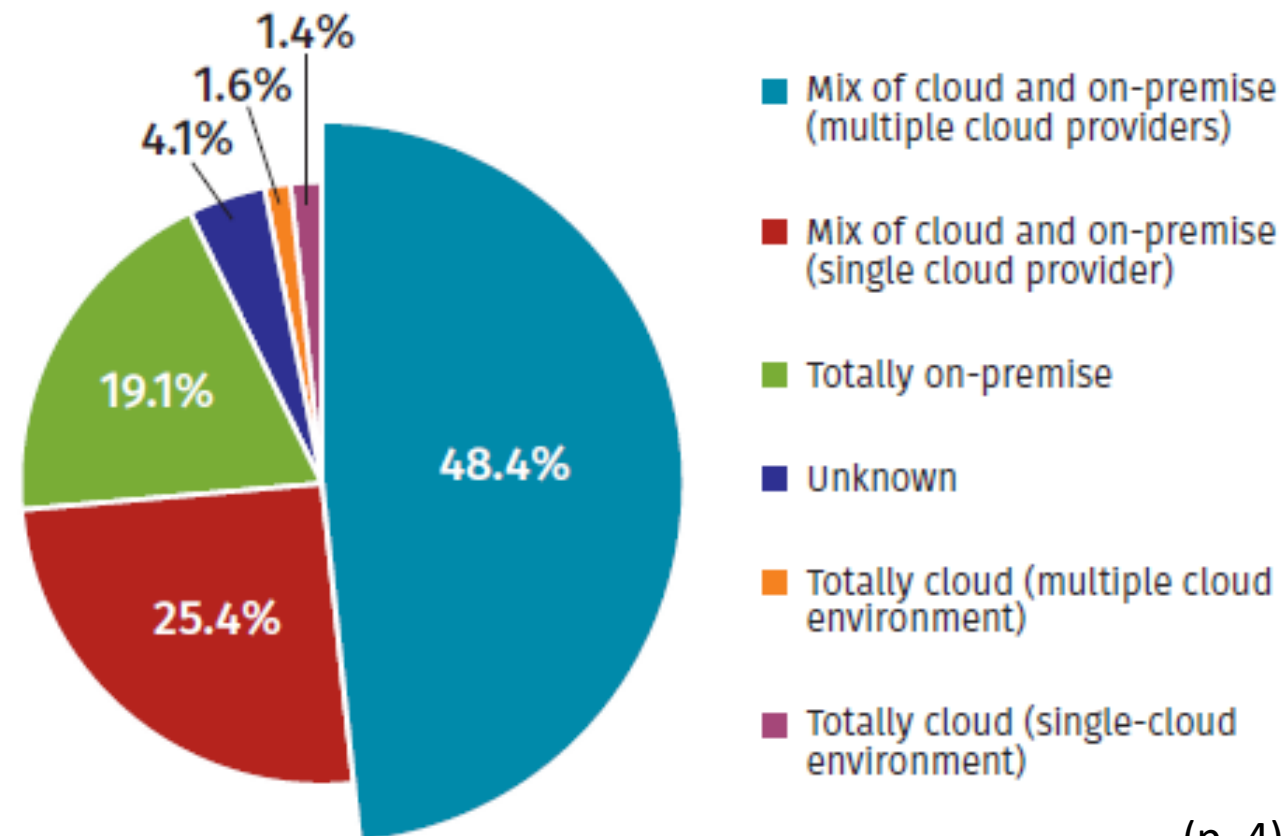
Matt Bromiley

Copyright SANS Institute 2020. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

<https://www.sans.org/white-papers/39105/>

What is the basic nature of your infrastructure?
Select the best choice.



(p. 4)

Poor Systems Engineering

Research Report

Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles

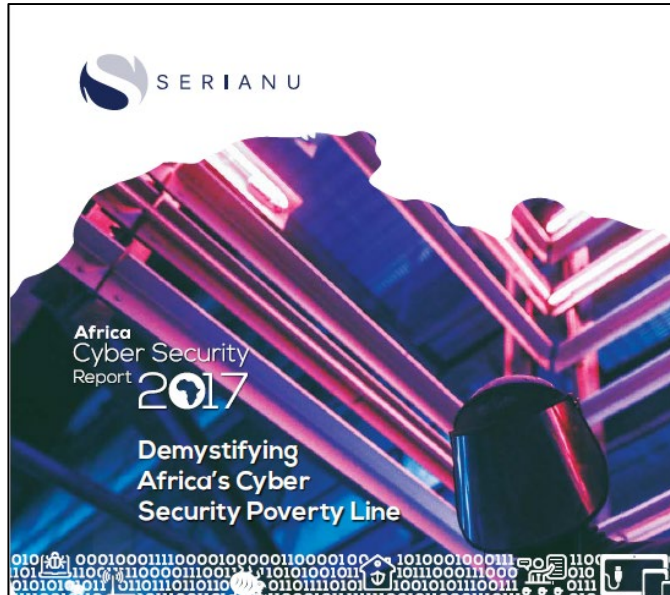
Don Snyder, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick, Michael H. Powell



“Poor system security engineering is very difficult to mitigate by overlaying security controls, whereas security controls overlaid on a sound, secure design can be quite effective. For systems that are fielded and no longer in production, design changes to improve cybersecurity generally necessitate a modification program and can be cost-prohibitive. Most Air Force systems reside in this “legacy” phase. It is especially important in this phase that a mission assurance perspective be adopted that examines the full spectrum of options for cybersecurity, including after-design protective measures, changes in operational procedures, and modifications, if necessary and affordable.” (Rand, p. 8)

https://www.rand.org/pubs/research_reports/RR1007.html

Cybersecurity Poverty Line



What is the cyber security poverty line?

Many organisations particularly SMEs lack the basic "commodities" that would assure them of the minimum security required and with the same analogy, be considered poor.

In the context of a cyber-security poverty line there are still numerous organisations particularly SMEs that do not have the skills, resources or funding to protect, detect and respond to cyber security threats. Many organisations and individuals fall below this line. We aim to demystify the cyber security poverty line within Africa.

(p. 9)



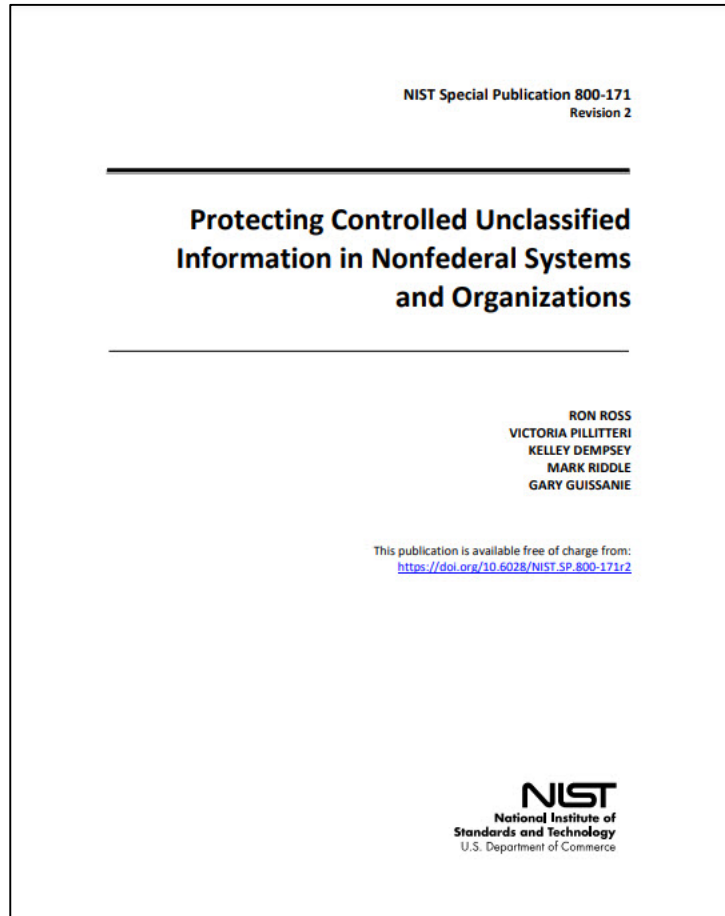
- Africa > 90% below poverty line
- Would you be below the cybersecurity poverty line?

General characteristics of organisations operating below the Cyber security poverty line are:

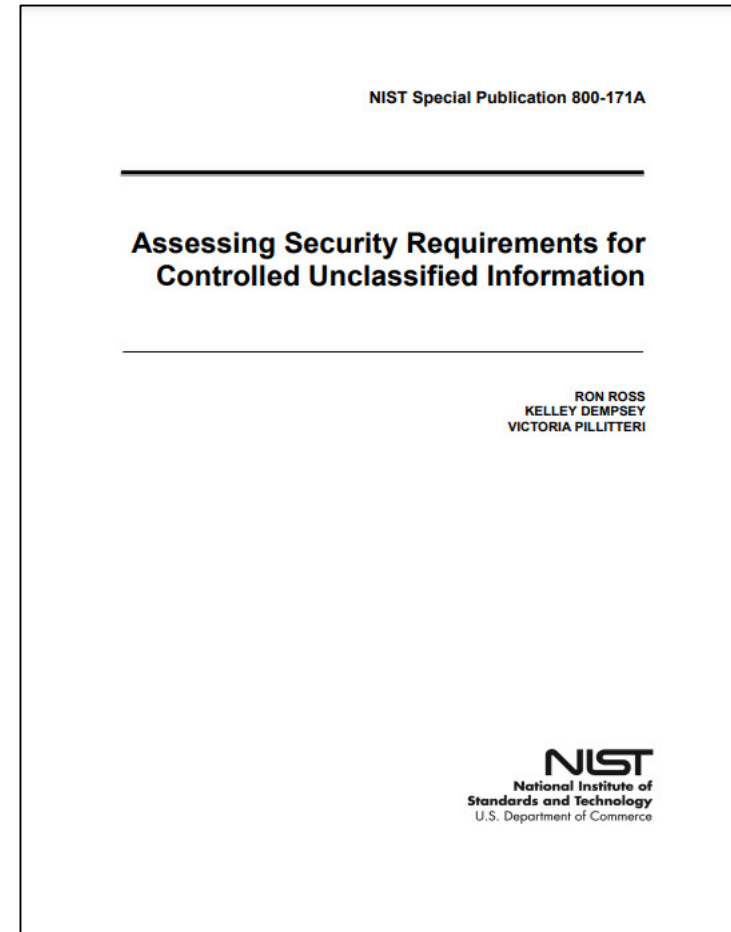
- Lack the minimum requirement for fending off an opportunistic adversary. → **Vulnerable to opportunistic attacker**
- Are essentially waiting to get taken down by an attack. → **Reactive response to attacks**
- There's also the idea of technical debt as a result of postponing important system updates. → **Postpones system updates**
- Lack in-house expertise to maintain a decent level of security controls and monitoring. → **Lacks expertise to maintain security controls**
- Tremendously dependent on third parties hence have less direct control over the security of the systems they use. → **Dependent upon 3rd parties for security**
- They also end up relinquishing risk decisions to third parties that they ideally should be making themselves. → **Relinquishes risk decisions to third parties**
- Lack resources to implement separate systems for different tasks, or different personnel to achieve segregation of duties. → **Lacks segmentation of duties**
- They'll use the cheapest software they can find regardless of its quality or security. → **Uses cheapest SW, regardless of security**
- They'll have all sorts of back doors to make administration easier for whoever they can convince to do it. → **Allows back doors to easy administrator tasks**

(p. 10)

NIST 800-171 & NIST 800-171A



<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>



<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf>

How are you doing

- Cyber Hygiene
- Security Controls
- Cyber Hardening
- Architecture
- Boundaries and Segmentation
- Resilience
- Other Security Techniques

What Makes Business Sense

How much and how often does your company need access to the sensitive information?

Best Practice: The fewer people and systems with access to sensitive information – generally the lower the cost and complexity of defense.

Do you have the ability to change the architecture of your network?

Best Practice: If limited ability to change your network architecture/design, you will gravitate to either an isolated network or an outsourced network.

Do you anticipate having either classified or highly sensitive unclassified information on your premise?

Best Practices: If you have to change to a higher threat level, you may need to redesign your network. If your facility is cleared for classified, it might be cheaper to put your highly sensitive unclassified information on the classified network.

Business Decision

How much & often does your company need access to the sensitive information?

- **Only a few people need occasional access**
- **Many people need regular access**

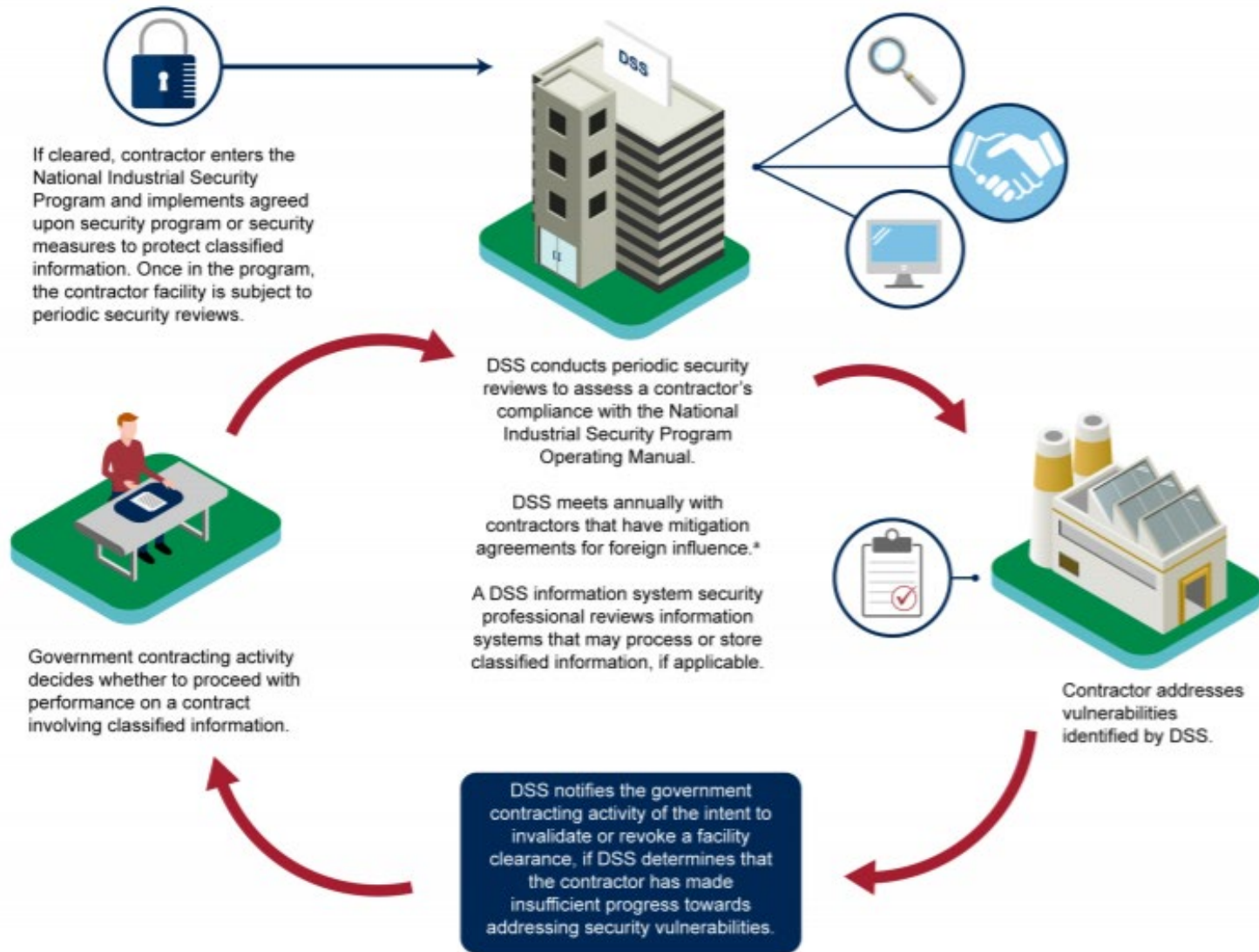
Do you have the ability to change the architecture of your network?

- **You have the ability to change your network architecture**
- **Network design is optimized for systems like an ERP or specialized systems**

Do you anticipate having either classified or highly sensitive unclassified information on your premise?

- **My CUI is mostly likely at a moderate Impact**
- **My CUI could easily become highly sensitive**

Cleared for Classified



When a site goes through the Cleared for Classified process – they have an approved transmission means, with acceptable storage, cleared personnel accessing the resources, are validated externally for set-up/operations, and are periodically audited by an external agency

Best Practice

A best practice for small businesses to limit investment cost is to limit sensitive unclassified information to a portion of their network or an enclave.

A “DIB contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.”

<https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of>

Cost Effective Security Considerations

Transmission – Accepted secure means of transmission. Objective is to minimize monitoring costs and minimize the threat's ability to compromise the confidentiality of the sensitive information.

Storage – Have a layered defense. Easy option is store as cyphertext and storage device has access controls. If storage is of cyphertext – it is not CUI until converted back to plaintext. Need to have ways of monitoring access to storage.

Access and Use/Modification – Minimize the number of devices and people with access. Do not retain CUI on the device, only on approved storage devices. As the device for access and use/modification are endpoints – best to use limited purpose and dedicated devices.

Monitoring – Skills for monitoring can widely vary. If your personnel need extensive analytical skills for log and threat analysis, costs can become very expensive, very quickly. Change in capability of the threat can dramatically increase your costs. Implemented security controls can easily follow S-cost curves (with additional incremental gains in capability coming at significant cost increases).

Choosing Between Designs

Questions to Work Through as a Business

How much and how often does your company need access to the sensitive information?

Do you have the ability to change the architecture of your network?

Do you anticipate having either classified or highly sensitive unclassified information on your premise?

Isolated Assets

Still have to transport Sensitive Information to network securely

Could add a burden to your people's work processes

Guard against insider threat

Connected Network

Connectivity to sensitive information, brings burden to increased attack surface

Need much better threat monitoring and vulnerability assessment – more capable analysts

External threat, insider threat, and supply chain threat.

Outsourced Network (Cloud as an example)

Dependent upon someone else and if contracted correctly

Leverage of other's capabilities – monitoring, threat analysis, vulnerability analysis

Incident response can be a big deal

Choices of Design

Isolated Assets

**Isolated (Air Gapped)
Controlled Access w/ Controls**

Advantages:

- Lower cost and faster to implement
- Requires less skill to manage
- Easier audit requirements

Disadvantages:

- Still susceptible to insider threat
- Could restrict business operations
- Over-confidence for air gap

Connected Network

**Onsite Network w/NIST 800-171/172
Security Requirements & Threat Service**

Advantages:

- Better alignment with business ops
- Easier to manage customer interface
- Some proven designs are effective (such as CMTC Stop Light Architecture)

Disadvantages:

- Requires extremely capable staff
- Costs of implementation and audit increase dramatically
- Increased probability of compromise, especially if threat changes

Outsourced Network (Cloud as an example)

Outsourced IT & Threat Service

Advantages:

- Leverage of provider's security
- Situational awareness and threat services
- Costs can be reduced

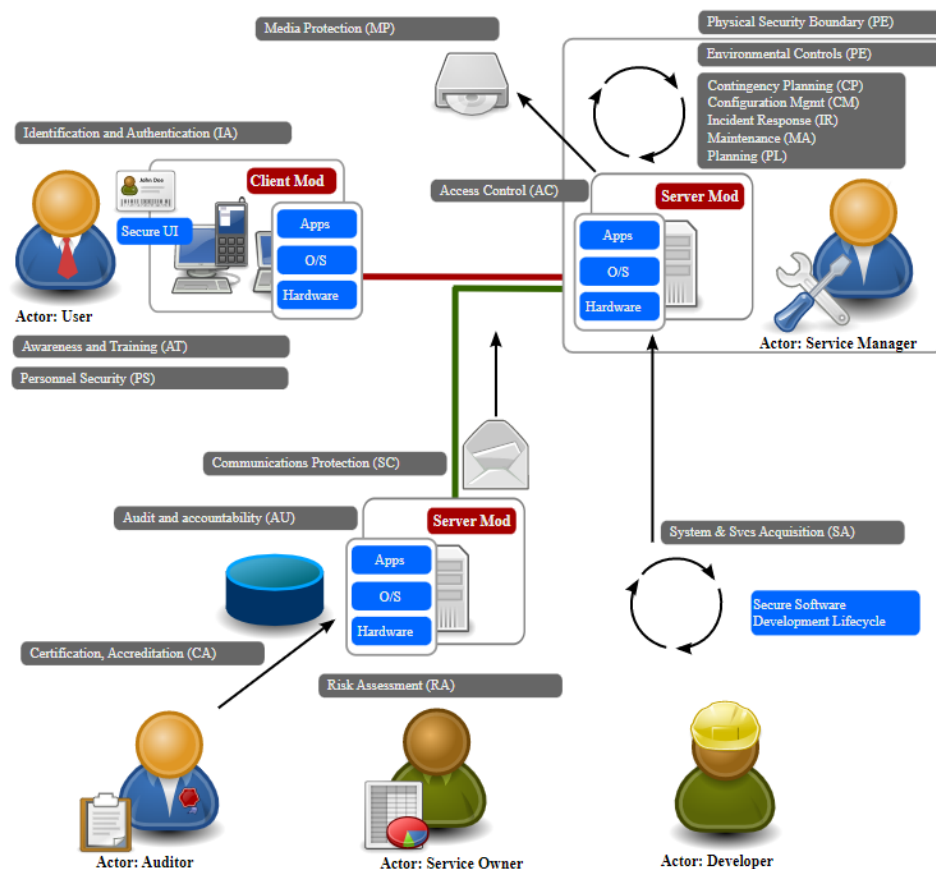
Disadvantages:

- Trust in provider required
- Third party risk
- Use of services accessible to public

Architecture – Generic Pattern

SP-009: Generic Pattern

Diagram: Example of a self contained Network



Description: The intention of this pattern is to show how the major control families apply to the computing environment. It aims to help familiarise people with the control families, and can provide a useful basis for thinking about security problems. This pattern can be used as the basis for other patterns. Users must authenticate in some manner to the systems they utilise. Server resources are managed to meet service level agreements. New services are periodically released into the environment. Existing services are maintained and decommissioned.

Assumptions: All computing systems are accessed from some form of user interface to a client. The client can connect to resources provided by a host across some form of network. Hosts can act as clients and servers to communicate. This model echoes the original design goals of TCP/IP where the intelligence is placed into the end point, and application layer of the network stack, and the network simply transfers data packets.”

<https://www.opensecurityarchitecture.org/cms/library/patternlandscape/236-0802pattern009>

Isolated Assets for Access & Storage

Provided as an example

Transmission - CD ROMs that are sent through the US Mail - double wrapped and appropriately marked. All data on the CD ROM are cyphertext. CD ROMs are destroyed after USPS receipt and cyphertext transferred to commercially bought AES 256-bit hardware encrypted hard drives. Different mail package for encryption keys.

Storage - Cyphertext stored on specific purpose AES 256-bit hardware encrypted hard drives (or encrypted thumb drives). One AES hard drive for CUI encrypted objects and one AES hard drive for crypto keys and downloaded transaction logs. The AES 256-bit hardware encrypted hard drive and any printed material will be stored at the SBIR's site in a sealed lockbox in a dedicated room (with no windows).

Access and Use - two air-gapped computers in controlled room that are appropriately monitored. Only authorized personnel are allowed in room. The computers use MFA to sign on. Two computers are connected by a cable – cable is to minimize tempest transmissions. One computer is for decrypting and viewing the cyphertext. The other computer is for recording logs and analyzing those logs. Both computers disable speakers and microphones to limit ultrasonic attacks and transmission. No retention of material is allowed on the viewing computer and all temporary files after viewing computer are purged. Other computer for logging required transactions and analyzing those transactions will periodically transfer files to the appropriate AES 256 bit encrypted hard drive. Both computers are periodically scanned for vulnerabilities and patched for updates of OS and critical software. Both computers use the DoD's STIG configurations for software and OS. All changes or updates of the CUI is done on those computers, stored on the AES 256-bit hard drives, and transmitted back to the customer as cyphertext with secure transmission.

Monitoring – Access to room and logs of viewing computer are analyzed. Provide validation that when cyphertext became plaintext (now is CUI) – that no retention on viewing computer and temporary files deleted. Need to prove that encryption keys are safely managed and not easily accessible with access to viewing computer.

Secure Storage

Store as Cyphertext – not Plaintext on a device that encrypts stored objects. This a layered defense of cyphertext being stored securely on a device that limits access and provides another layer of defense.

Example - commercially bought AES 256-bit hardware encrypted hard drives and thumb drives



Note: the above images are purely representational and not an endorsement of a specific product

AF Digital Strategy

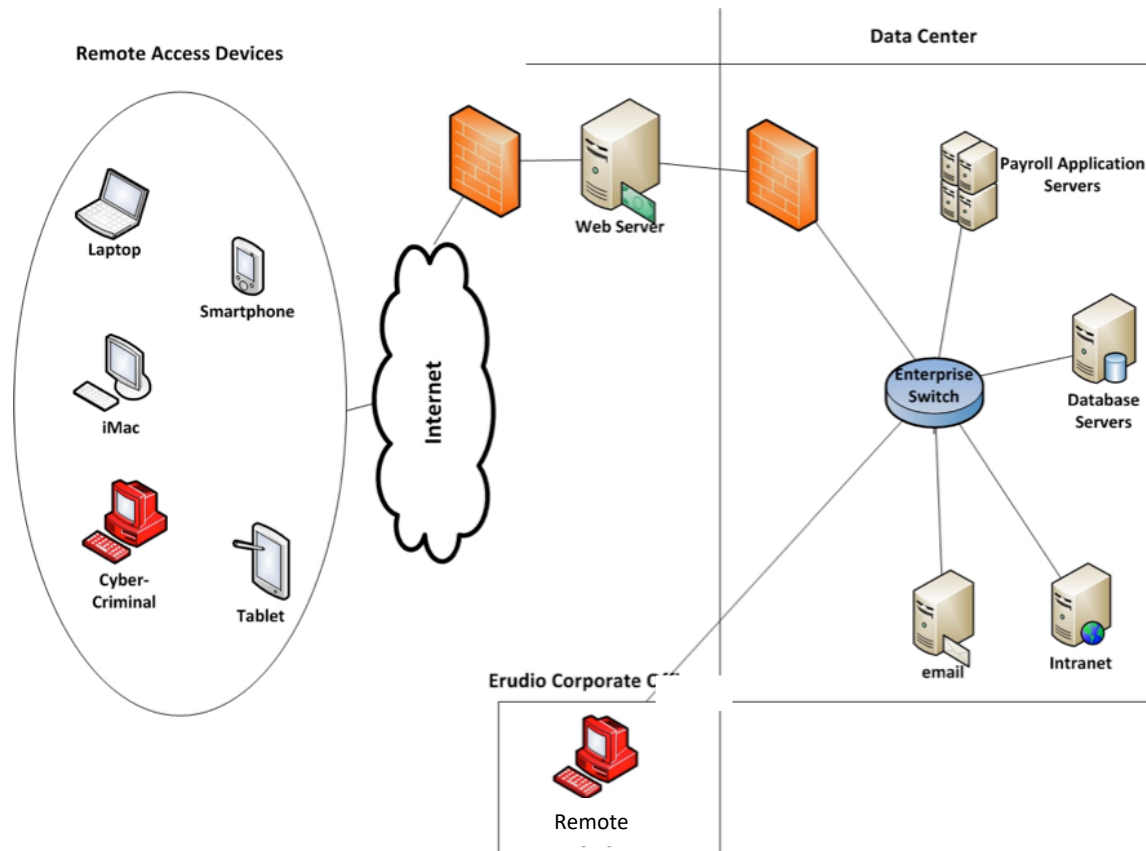


“Mr. Caron compared legacy networks, most of which are architected as flat networks, to Tootsie Roll Pops, with a “hard outer shell with a soft, gooey center” —once adversaries find an opening in the perimeter security, they can leverage vulnerabilities and gain full access. Many efforts have been made to prevent such breaches, but, referencing Frederick the Great, he said that “he who defends everything defends nothing.” He asserted that trying to protect all systems, applications, and data equally leads to a situation in which some are overprotected, others are underprotected, and overall network functionality is constrained. Instead, the optimal approach to cybersecurity is to determine where protections are needed based on the sensitivity and associated risk of individual components.” (p. 48 -49)

<https://nap.nationalacademies.org/catalog/26531/digital-strategy-for-the-department-of-the-air-force-proceedings>

Architecture – flat network

Network connected to outside world



NEWS

Target breach happened because of a basic network segmentation error

Hackers gained access to Target POS systems using login credentials belonging to an HVAC company

According to Krebs, sources close to the investigation said the attackers first gained access to Target's network on Nov. 15, 2013 with a username and password stolen from Fazio Mechanical Services, a Sharpsburg, Pa.-based company that specializes in providing refrigeration and HVAC systems for companies like Target.

Fazio apparently had access rights to Target's network for carrying out tasks like remotely monitoring energy consumption and temperatures at various stores.

The attackers leveraged the access provided by the Fazio credentials to move about undetected on Target's network and upload malware programs on the company's Point of Sale (POS) systems.

Available at <http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html>

Why a flat network is so common and extremely insecure

- Simple to architect
- Cheap to build
- Easy to operate and maintain

What is the right balance between ease of use and security?

Flat Network = Bad



UNITED STATES COAST GUARD
U.S. Department of Homeland Security

MARINE SAFETY ALERT

Inspections and Compliance Directorate

July 8, 2019
Washington, D.C.

Safety Alert 06-19

Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels

In February 2019, a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were experiencing a significant cyber incident impacting their shipboard network. An interagency team of cyber experts, led by the Coast Guard, responded and conducted an analysis of the vessel's network and essential control systems. The team concluded that although the malware significantly degraded the functionality of the onboard computer system, essential vessel control systems had not been impacted. Nevertheless, the interagency response found that the vessel was operating without effective cybersecurity measures in place, exposing critical vessel control systems to significant vulnerabilities.

Prior to the incident, the security risk presented by the shipboard network was well known among the crew. Although most crewmembers didn't use onboard computers to check personal email, make online purchases or check their bank accounts, the same shipboard network was used for official business – to update electronic charts, manage cargo data and communicate with shore-side facilities, pilots, agents, and the Coast Guard.

It is unknown whether this vessel is representative of the current state of cybersecurity aboard deep draft vessels. However, with engines that are controlled by mouse clicks, and growing reliance on electronic charting and navigation systems, protecting these systems with proper cybersecurity measures is as essential as controlling physical access to the ship or performing routine maintenance on traditional machinery. It is imperative that the maritime community adapt to changing technologies and the changing threat landscape by recognizing the need for and implementing basic cyber hygiene measures.

In order to improve the resilience of vessels and facilities, and to protect the safety of the waterways in which they operate, the U.S. Coast Guard strongly recommends that vessel and facility owners, operators and other responsible parties take the following basic measures to improve their cybersecurity:

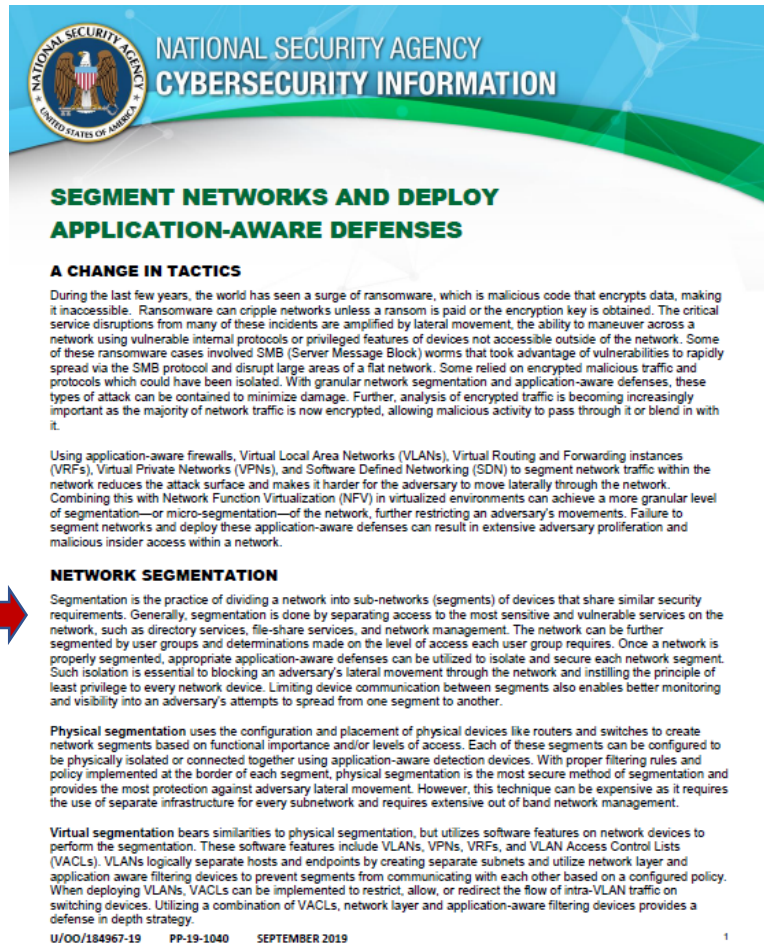
- **Segment Networks.** "Flat" networks allow an adversary to easily maneuver to any system connected to that network. Segment your networks into "subnetworks" to make it harder for an adversary to gain access to essential systems and equipment.
- **Per-user Profiles & Passwords.** Eliminate the use of generic log-in credentials for multiple personnel. Create network profiles for each employee. Require employees to enter a password and/or insert an ID card to log on to onboard equipment. Limit access/privileges to only those levels necessary to allow each user to do his or her job. Administrator accounts should be used sparingly and only when necessary.

1

““Flat” networks allow an adversary to easily maneuver to any system connected to that network. Segment your networks into “subnetworks” to make it harder for an adversary to gain access to essential systems and equipment.”

<https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf>

Segment Networks



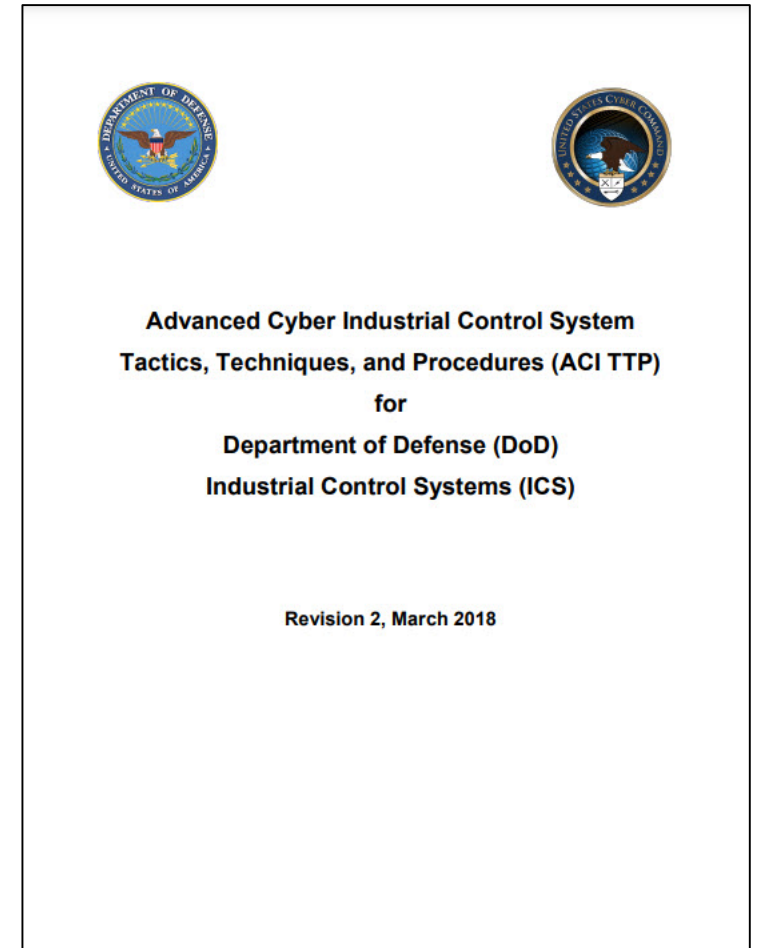
“Segmentation is the practice of dividing a network into sub-networks (segments) of devices that share similar security requirements. Generally, segmentation is done by separating access to the most sensitive and vulnerable services on the network, such as directory services, file-share services, and network management. The network can be further segmented by user groups and determinations made on the level of access each user group requires. Once a network is properly segmented, appropriate application-aware defenses can be utilized to isolate and secure each network segment. Such isolation is essential to blocking an adversary’s lateral movement through the network and instilling the principle of least privilege to every network device. Limiting device communication between segments also enables better monitoring and visibility into an adversary’s attempts to spread from one segment to another.” (p. 1)

<https://media.defense.gov/2019/Sep/09/2002180325/-1/-1/0/Segment%20Networks%20and%20Deploy%20Application%20Aware%20Defenses%20-%20Copy.pdf>

Segmentation Strategy

Creating a Segmentation Strategy

- “a. The segmentation strategy is a documented process for understanding how your ICS assets could be separated during and after a cyber attack. Each ICS environment is unique, based on protocols, network architecture, physical locations, equipment, software, and mission priorities.
- b. The first step is to identify the commander’s mission priorities. These are the most critical processes that must remain operational.
- c. The second step is to identify critical processes and dependencies. This includes identifying all of the assets that are required to keep the mission priorities operational.
- d. The third step is to review the network architecture to identify logical points where segmentation could occur to contain infected assets or protect the ICS processes.
- e. This document should be maintained with the continuity of operations and baseline documentation.” (p. H-1)

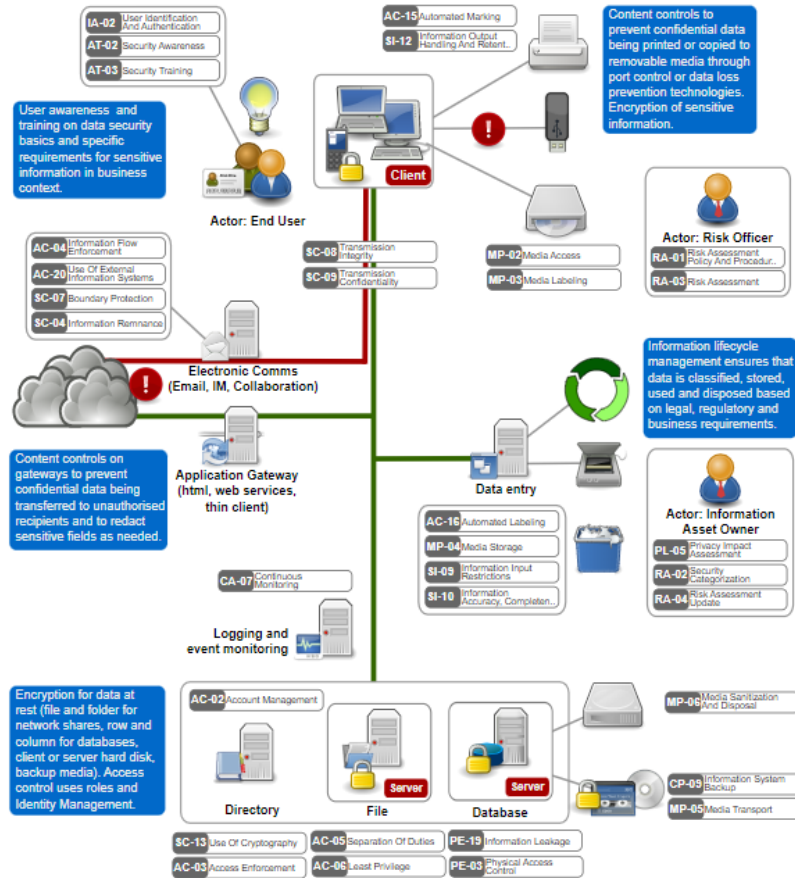


<https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/DoD-Advanced-Cyber-Industrial-Control-System-Tactics-Techniques-and-Procedures-ACI-TTP>

Architecture – Data Security

SP-013: Data Security Pattern

Diagram:



06_02_Pattern_013_02_DataSecurity.svg
 OSA is licensed according to Creative Commons Share-alike.
 Please see: <http://www.opensecurityarchitecture.org/cms/community/license-terms>

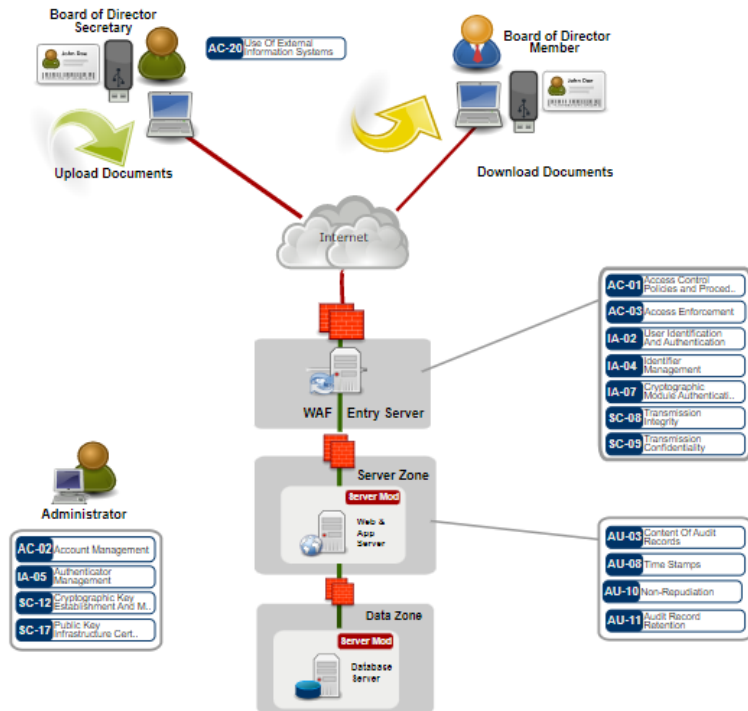
“A Data Classification scheme is often used to help understand which controls are needed for the data types processed by the organisation. This scheme will be defined based on the legal, regulatory and business requirements that the organisation must adhere. Common schemes used have 3 or 4 levels, including Public/Unclassified (e.g. Marketing materials), Internal Use (Information shared within the organisation or with suppliers e.g. Intranet), Confidential/Private (Sensitive information e.g. Credit card details or Medical history), Secret (Market Sensitive Information e.g Year-end results or Secret recipe for Coca-Cola).”

<https://www.opensecurityarchitecture.org/cms/library/patternlandscape/259-pattern-data-security>

Architecture – Secure Access

SP-022: Board of Directors Room

Diagram:

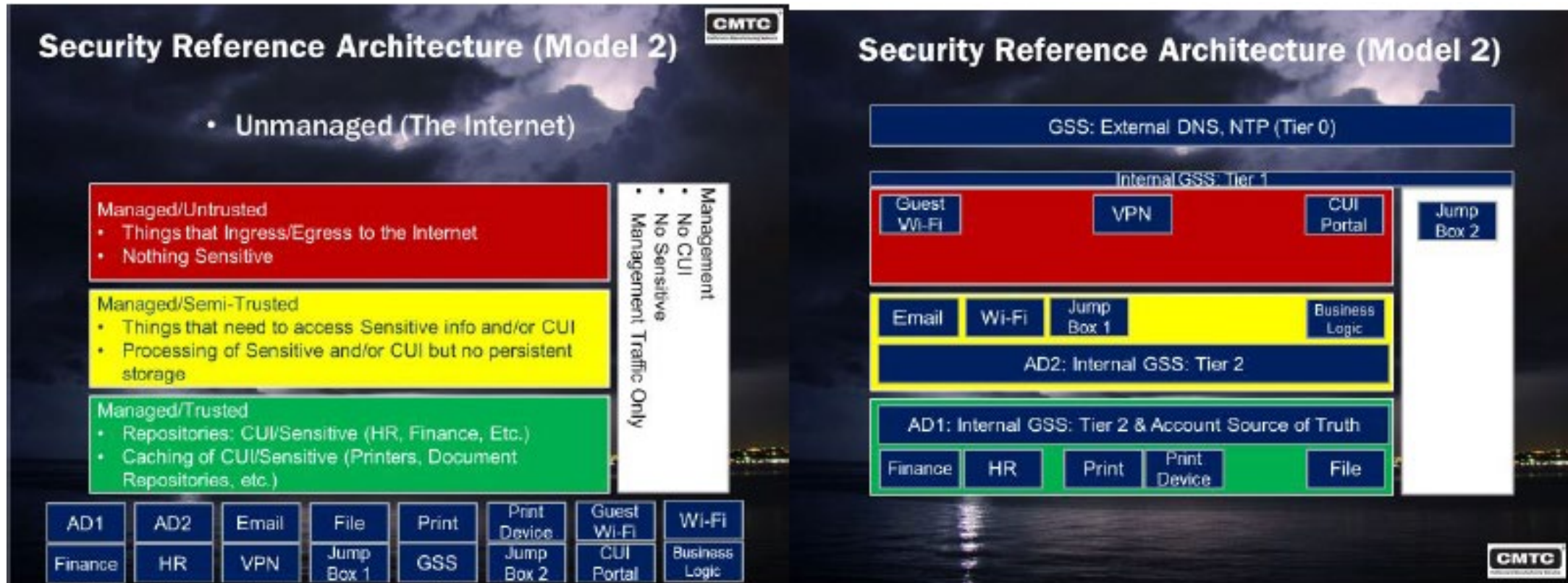


“Synopsis: Board of Directors Room for reading highly confidential documents on an un-trusted computer.

Description: Board of Directors need access to meeting protocols, agenda and other highly confidential information. Any computer may be used, even un-trusted or compromised computers. The documents accessible are highly confidential and no traces of documents shall be found on computer. It shall not be possible to download the documents in clear text or to print the documents. Detailed audit functionality shows which user has read which document and when. All documents are stored in the PDF format.”

<https://www.opensecurityarchitecture.org/cms/library/patternlandscape/292-pattern-board-room>

Scenario 2: Connected Network



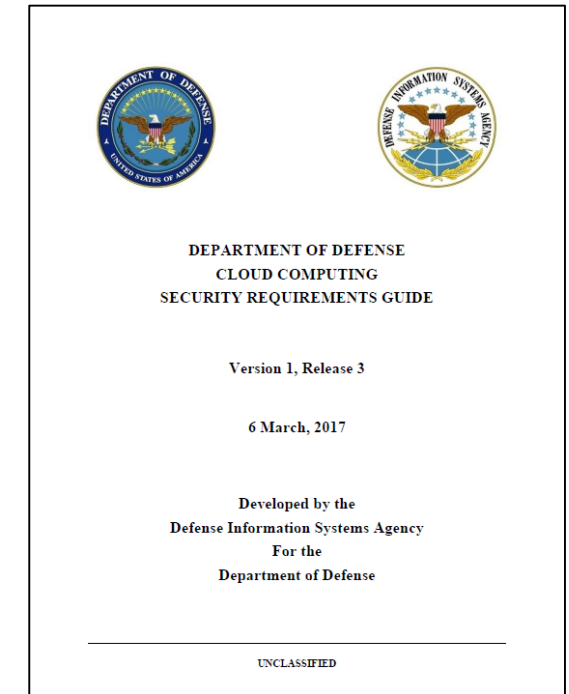
<https://www.cmtc.com/cybersecurity>

Scenario 3: Outsourced (Cloud) Networking

- All DoD data is important, but not all data needs to be equally protected
- Information Impact Levels (IILs) consider the potential impact should the confidentiality and integrity of the information be compromised

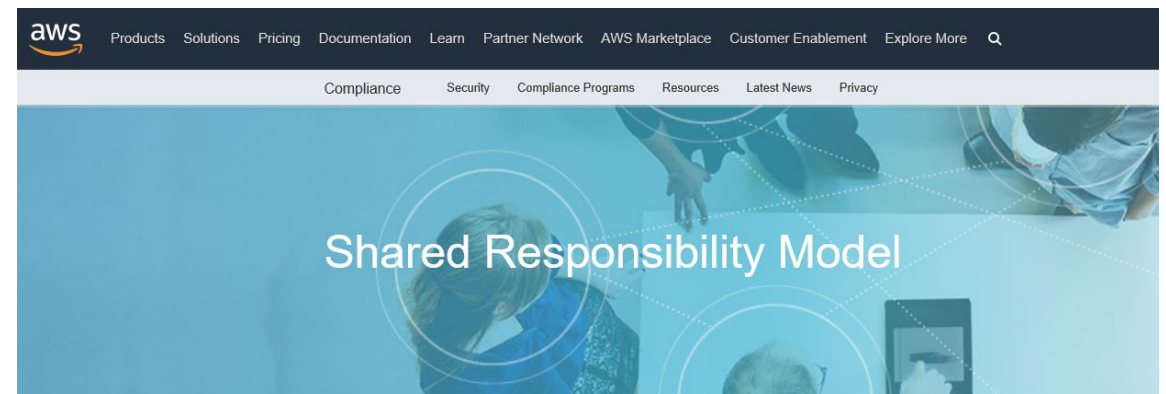
IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

CUI is at least IIL 4 or above!!



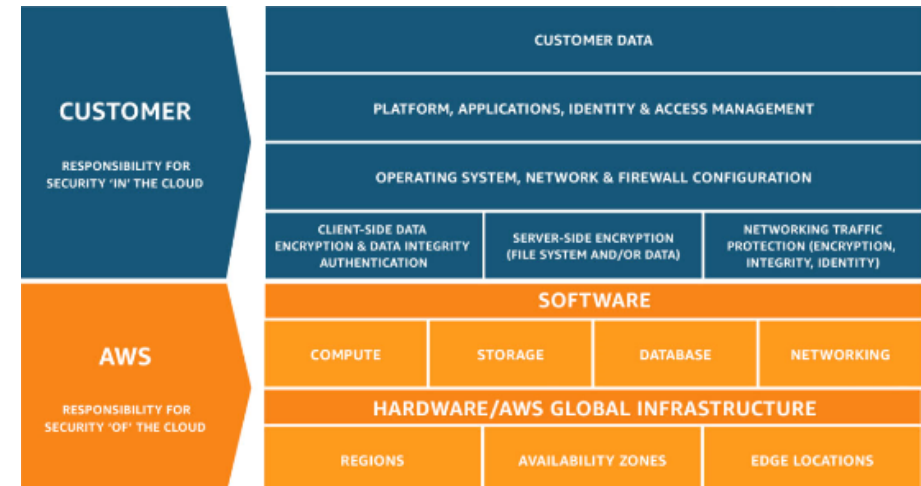
Shared Responsibility

<https://aws.amazon.com/compliance/shared-responsibility-model/>



"Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud."

..."This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation and verification of IT controls shared. AWS can help relieve customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment."



Questions