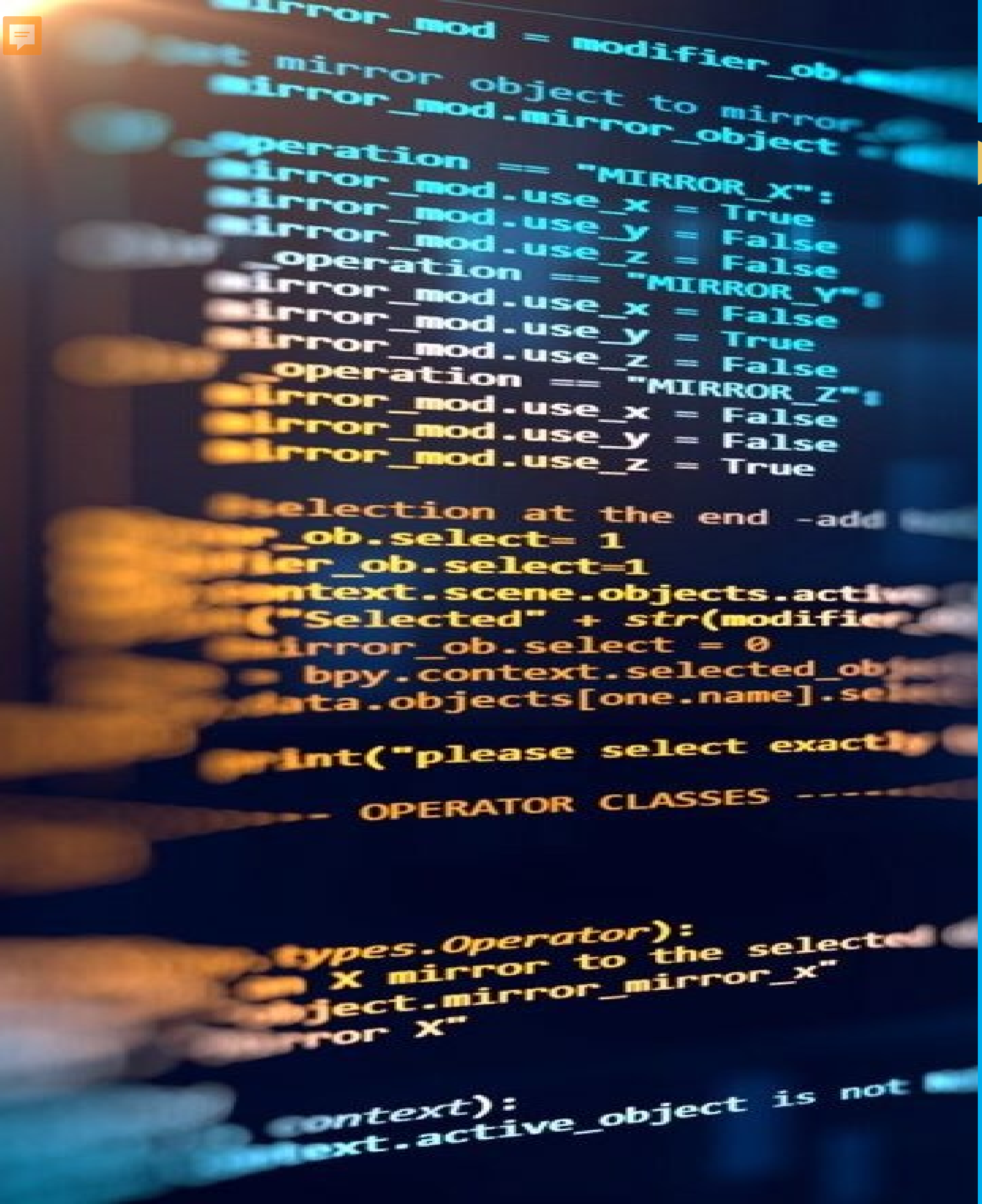


AN OFFERING IN THE DEEP BLUE CYBER SERIES

Zero Trust Concepts:

Cost Effective Cybersecurity (Part 2)

VERSION: NOVEMBER 2022

#30 IN THE DEEP BLUE CYBER EDUCATION SERIES

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2021-3218, 22 September 2021.

DAU

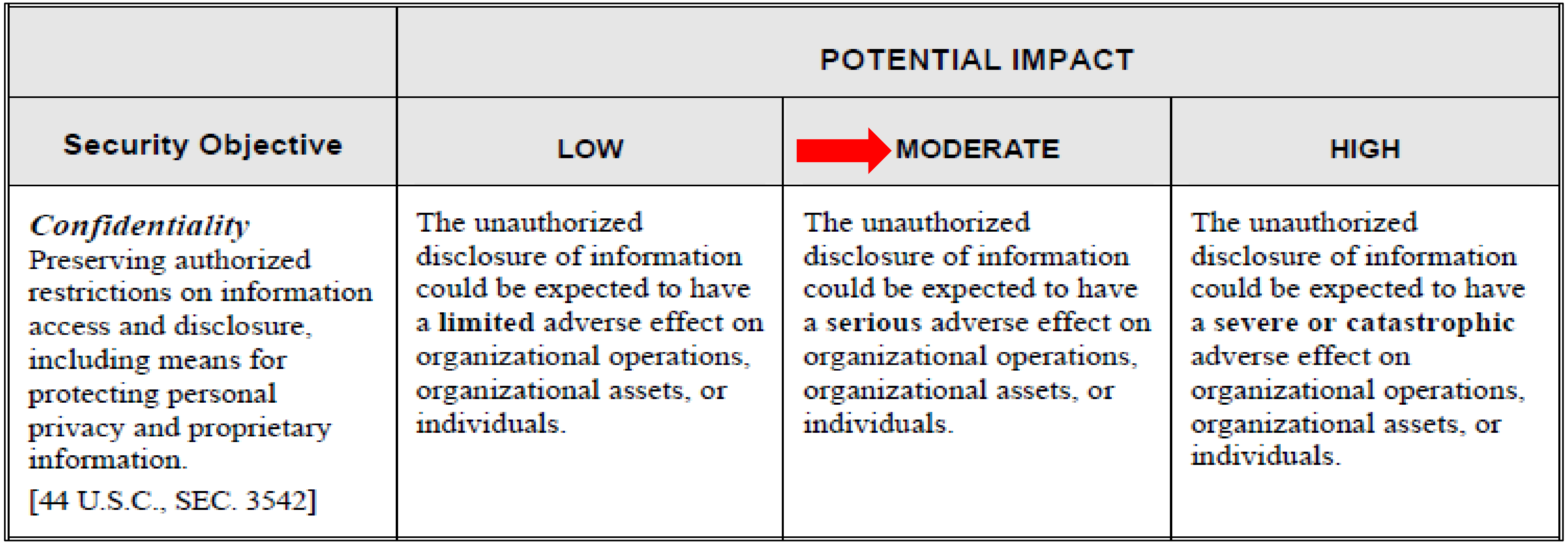
Cost Effective Cybersecurity (Part 2): Zero Trust Concepts

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

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Potential Impact

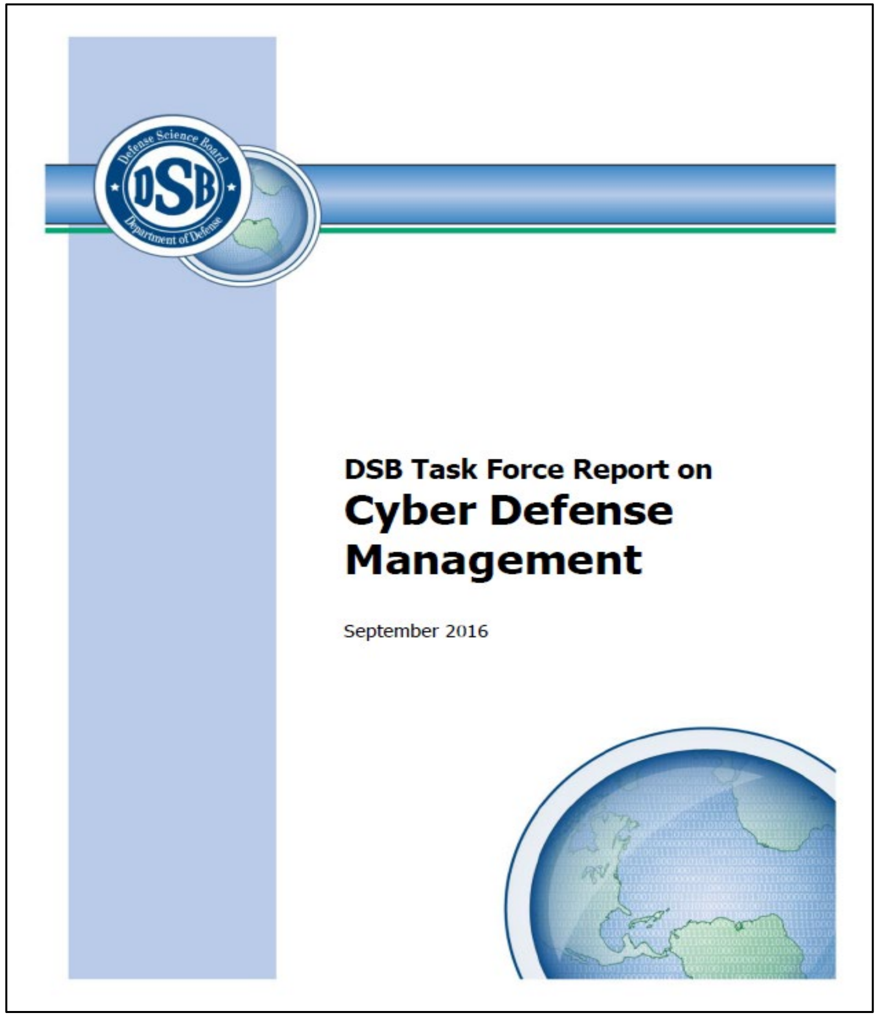
“With regard to *federal information systems*, requirements in the federal regulation for protecting CUI at the moderate confidentiality impact level will be based on applicable policies established by OMB and applicable government wide standards and guidelines issued by NIST.” NIST 171 r1, p. v



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality 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.

FIPS 199, p. 6

Basic CYBER Investments



DSB Task Force Report on

Cyber Defense Management

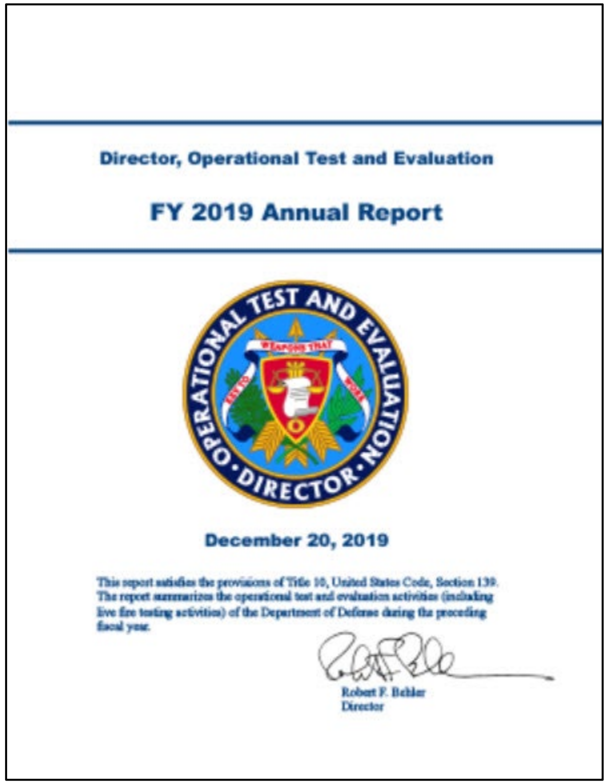
September 2016

"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.



Director, Operational Test and Evaluation

FY 2019 Annual Report

December 20, 2019

This report satisfies the provisions of Title 10, United States Code, Section 139. The report summarizes the operational test and evaluation activities (including live fire testing activities) of the Department of Defense during the preceding fiscal year.

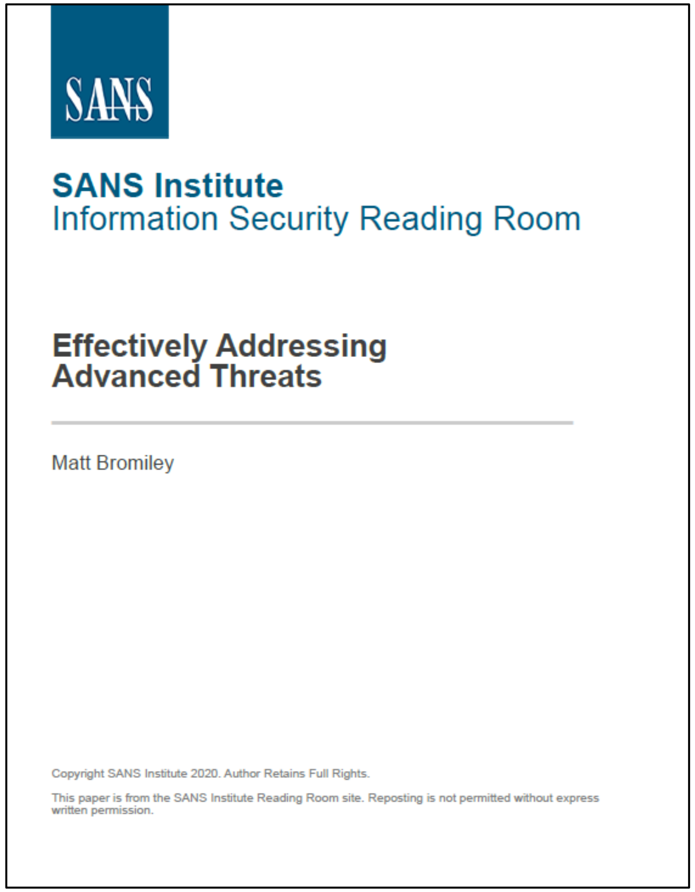
Robert F. Behler
Director

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

"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)

Your Environment



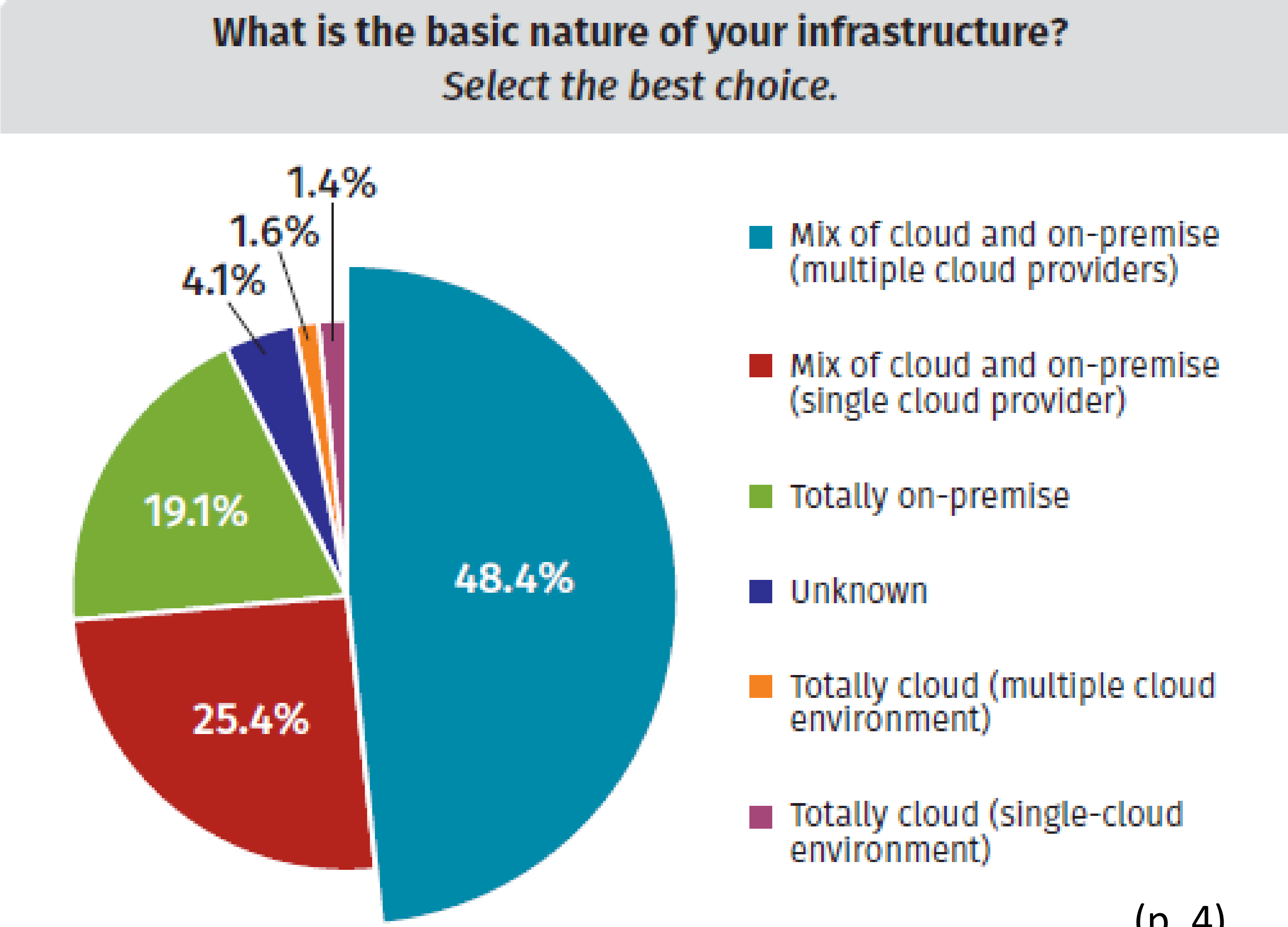
SANS

SANS Institute
Information Security Reading Room

Effectively Addressing Advanced Threats

Matt Bromiley

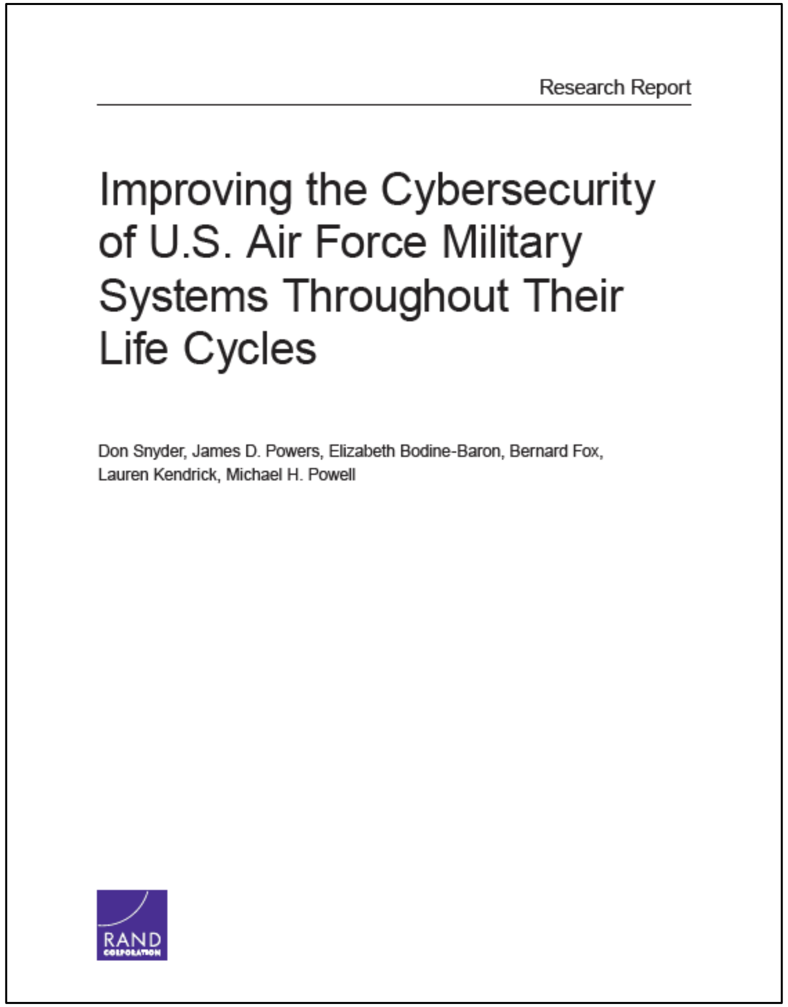
https://www.sans.org/white-papers/39105/



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

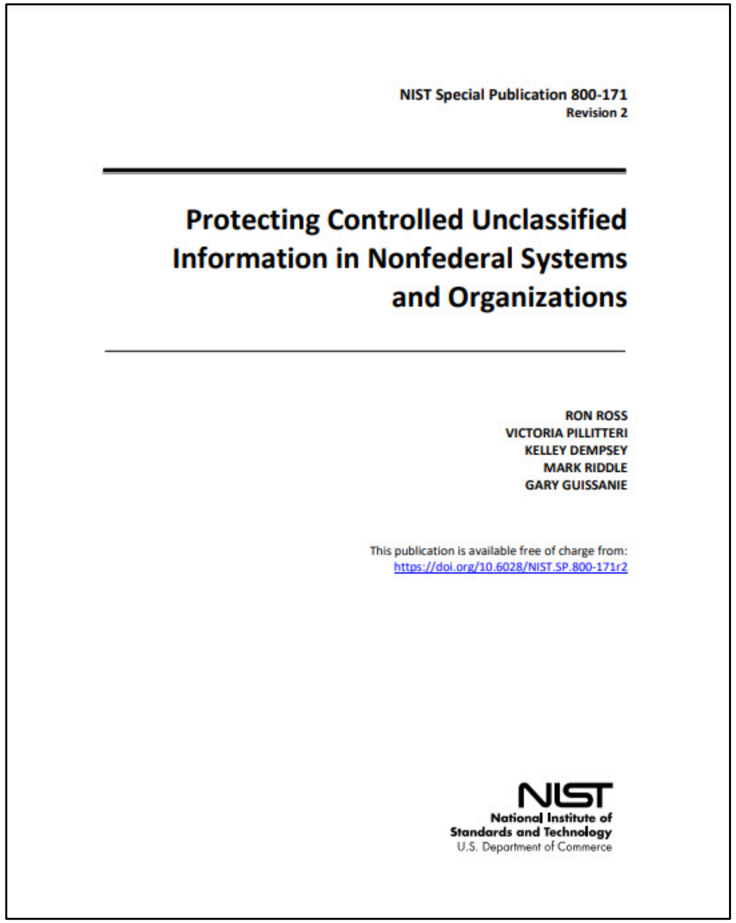
Don Snyder, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick, Michael H. Powell

RAND CORPORATION

"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

NIST 800-171 & NIST 800-171A



NIST Special Publication 800-171
Revision 2

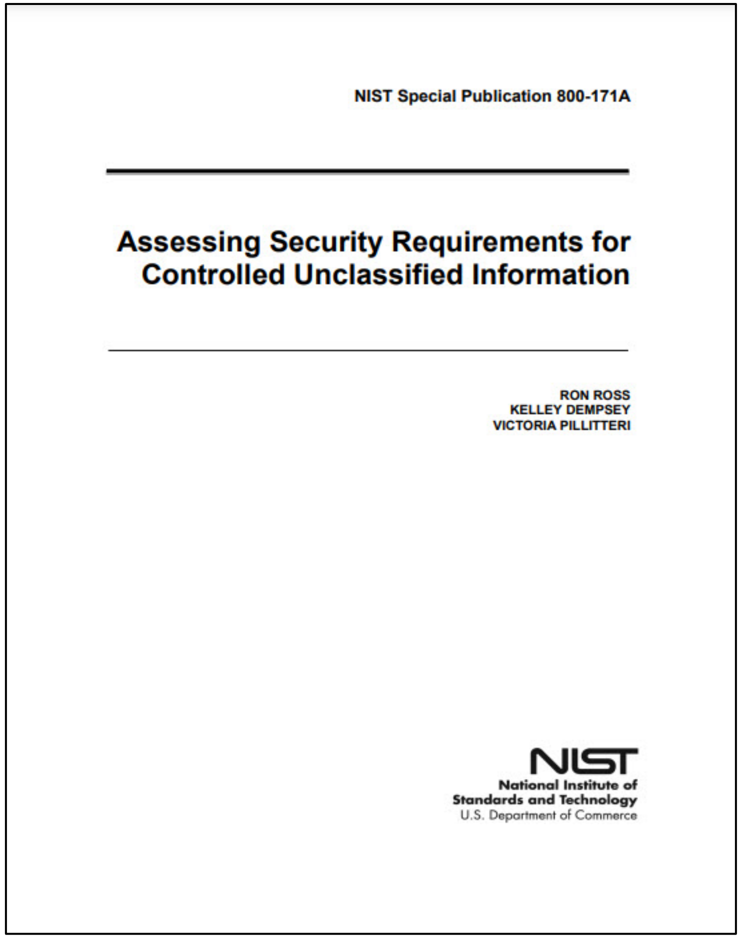
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

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



NIST Special Publication 800-171A

Assessing Security Requirements for Controlled Unclassified Information

RON ROSS
KELLEY DEMPSEY
VICTORIA PILLITTERI

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

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

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.

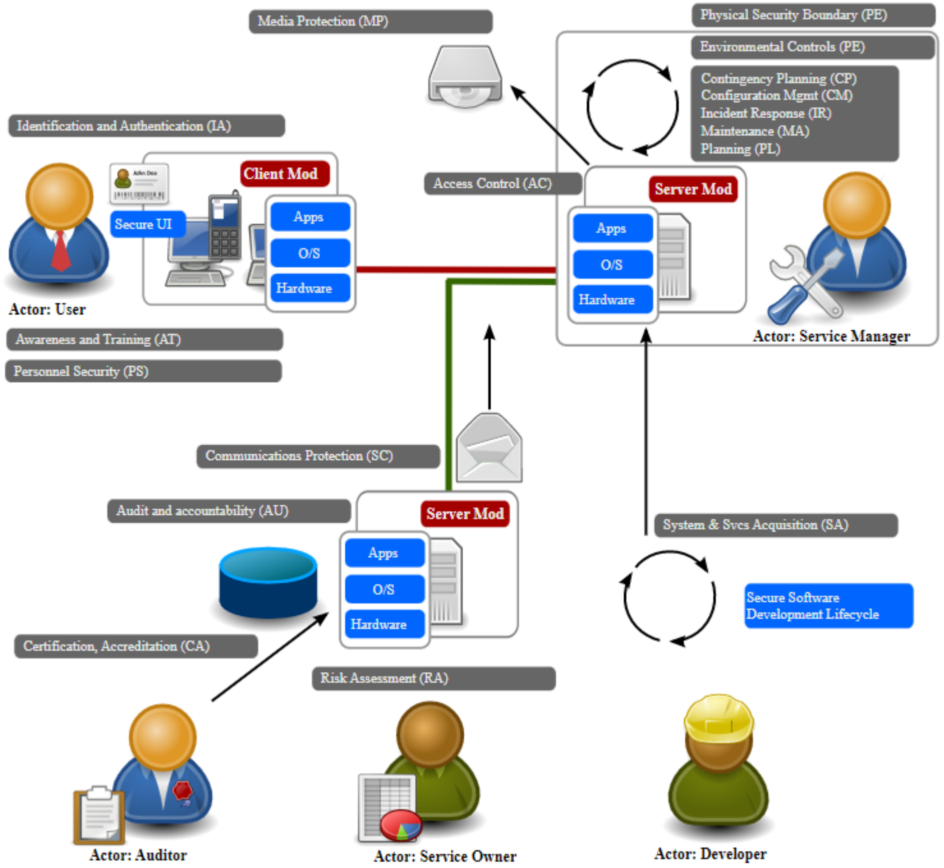
Access and Use/Modification – Minimize the number of devices and people with access. Do not retain CUI on the device, only on approved storage devices. As the device for access and use/modification are endpoints – best to use limited purpose and dedicated devices.

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).

Architecture – Generic Pattern

SP-009: Generic Pattern

Diagram: **Example of a self contained Network**

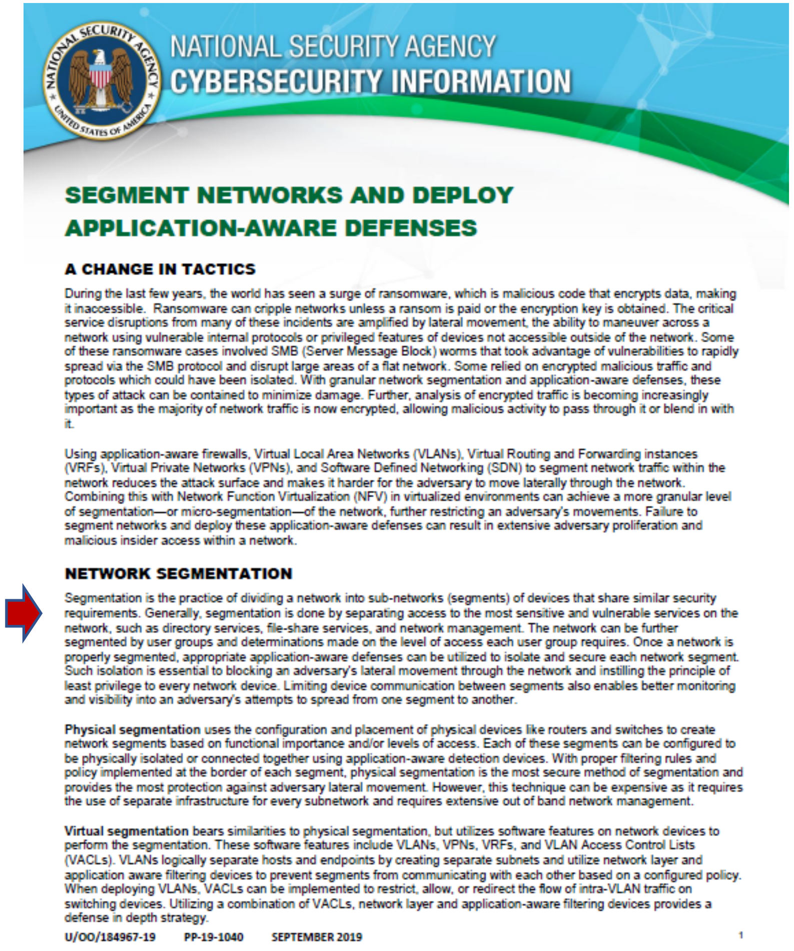


https://www.opensecurityarchitecture.org/cms/library/patternlandscape/236-0802pattern009

“**Description**: The intention of this pattern is to show how the major control families apply to the computing environment. It aims to help familiarize 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 utilize. 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.”

Segment Networks



NATIONAL SECURITY AGENCY
CYBERSECURITY INFORMATION

SEGMENT NETWORKS AND DEPLOY APPLICATION-AWARE DEFENSES

A CHANGE IN TACTICS

During the last few years, the world has seen a surge of ransomware, which is malicious code that encrypts data, making it inaccessible. Ransomware can cripple networks unless a ransom is paid or the encryption key is obtained. The critical service disruptions from many of these incidents are amplified by lateral movement, the ability to maneuver across a network using vulnerable internal protocols or privileged features of devices not accessible outside of the network. Some of these ransomware cases involved SMB (Server Message Block) worms that took advantage of vulnerabilities to rapidly spread via the SMB protocol and disrupt large areas of a flat network. Some relied on encrypted malicious traffic and protocols which could have been isolated. With granular network segmentation and application-aware defenses, these types of attack can be contained to minimize damage. Further, analysis of encrypted traffic is becoming increasingly important as the majority of network traffic is now encrypted, allowing malicious activity to pass through it or blend in with it.

Using application-aware firewalls, Virtual Local Area Networks (VLANs), Virtual Routing and Forwarding instances (VRFs), Virtual Private Networks (VPNs), and Software Defined Networking (SDN) to segment network traffic within the network reduces the attack surface and makes it harder for the adversary to move laterally through the network. Combining this with Network Function Virtualization (NFV) in virtualized environments can achieve a more granular level of segmentation—or micro-segmentation—of the network, further restricting an adversary's movements. Failure to segment networks and deploy these application-aware defenses can result in extensive adversary proliferation and malicious insider access within a network.

NETWORK SEGMENTATION

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.

Physical segmentation uses the configuration and placement of physical devices like routers and switches to create network segments based on functional importance and/or levels of access. Each of these segments can be configured to be physically isolated or connected together using application-aware detection devices. With proper filtering rules and policy implemented at the border of each segment, physical segmentation is the most secure method of segmentation and provides the most protection against adversary lateral movement. However, this technique can be expensive as it requires the use of separate infrastructure for every subnetwork and requires extensive out of band network management.

Virtual segmentation bears similarities to physical segmentation, but utilizes software features on network devices to perform the segmentation. These software features include VLANs, VPNs, VRFs, and VLAN Access Control Lists (VACLs). VLANs logically separate hosts and endpoints by creating separate subnets and utilize network layer and application aware filtering devices to prevent segments from communicating with each other based on a configured policy. When deploying VLANs, VACLs can be implemented to restrict, allow, or redirect the flow of intra-VLAN traffic on switching devices. Utilizing a combination of VACLs, network layer and application-aware filtering devices provides a defense in depth strategy.

U/OO/184967-19 PP-19-1040 SEPTEMBER 2019 1

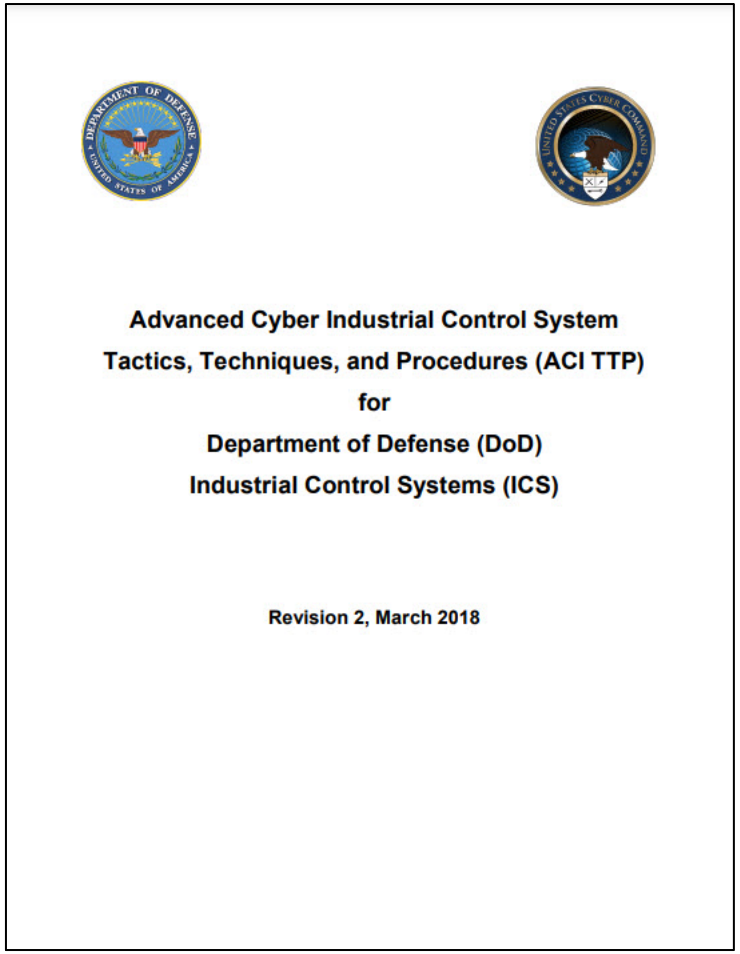
"Segmentation is the practice of dividing a network into sub-networks (segments) of devices that share similar security requirements. Generally, segmentation is done by separating access to the most sensitive and vulnerable services on the network, such as directory services, file-share services, and 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)



Advanced Cyber Industrial Control System
Tactics, Techniques, and Procedures (ACI TTP)
for
Department of Defense (DoD)
Industrial Control Systems (ICS)

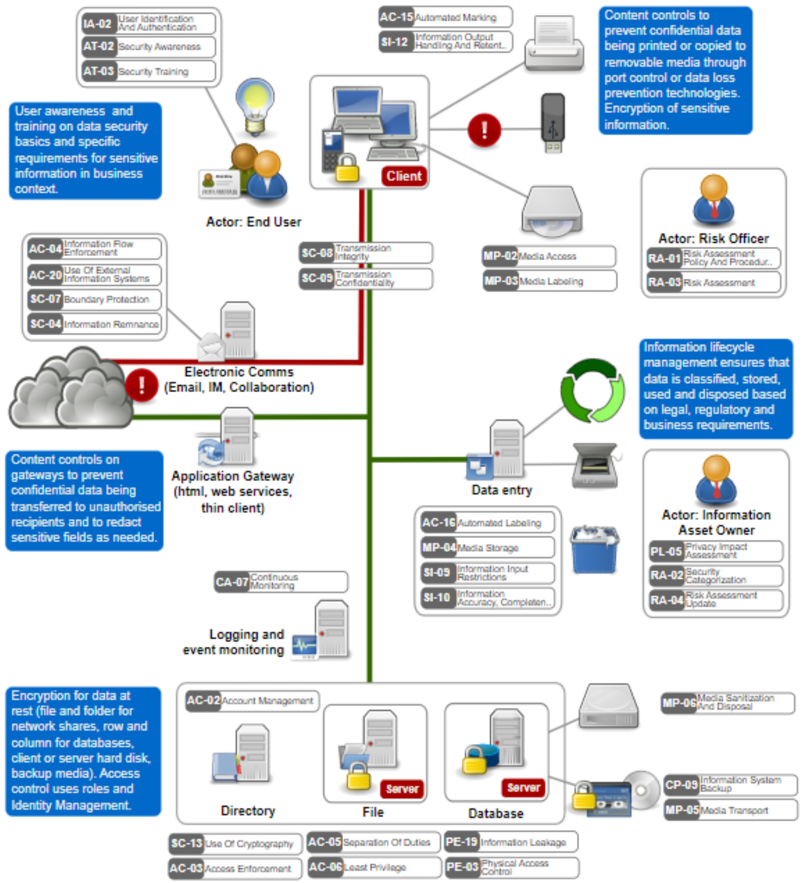
Revision 2, March 2018

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:


IA-02 User Identification And Authentication
AT-02 Security Awareness
AT-03 Security Training
AC-15 Automated Marking
SI-12 Information Output Handling And Retent..
Actor: End User
Client
!
Actor: Risk Officer
RA-01 Risk Assessment Policy And Procedur..
RA-03 Risk Assessment
AC-04 Information Flow Enforcement
AC-20 Use Of External Information Systems
SC-07 Boundary Protection
SC-04 Information Remnance
SC-08 Transmission Integrity
SC-09 Transmission Confidentiality
MP-02 Media Access
MP-03 Media Labeling
Electronic Comms (Email, IM, Collaboration)
!
Application Gateway (html, web services, thin client)
Data entry
Actor: Information Asset Owner
PL-05 Privacy Impact Assessment
RA-02 Security Categorization
RA-04 Risk Assessment Update
AC-16 Automated Labeling
MP-04 Media Storage
SI-09 Information Input Restrictions
SI-10 Information Accuracy, Completen..
CA-07 Continuous Monitoring
Logging and event monitoring
AC-02 Account Management
Directory
Server
File
Server
Database
MP-06 Media Sanitization And Disposal
CP-09 Information System Backup
MP-05 Media Transport
SC-13 Use Of Cryptography
AC-03 Access Enforcement
AC-05 Separation Of Duties
AC-06 Least Privilege
PE-19 Information Leakage
PE-03 Physical Access Control

User awareness and training on data security basics and specific requirements for sensitive information in business context.

Content controls to prevent confidential data being printed or copied to removable media through port control or data loss prevention technologies. Encryption of sensitive information.

Information lifecycle management ensures that data is classified, stored, used and disposed based on legal, regulatory and business requirements.

Content controls on gateways to prevent confidential data being transferred to unauthorised recipients and to redact sensitive fields as needed.

Encryption for data at rest (file and folder for network shares, row and column for databases, client or server hard disk, backup media). Access control uses roles and Identity Management.

08_02_Pattern_013_02_DataSecurity.svg

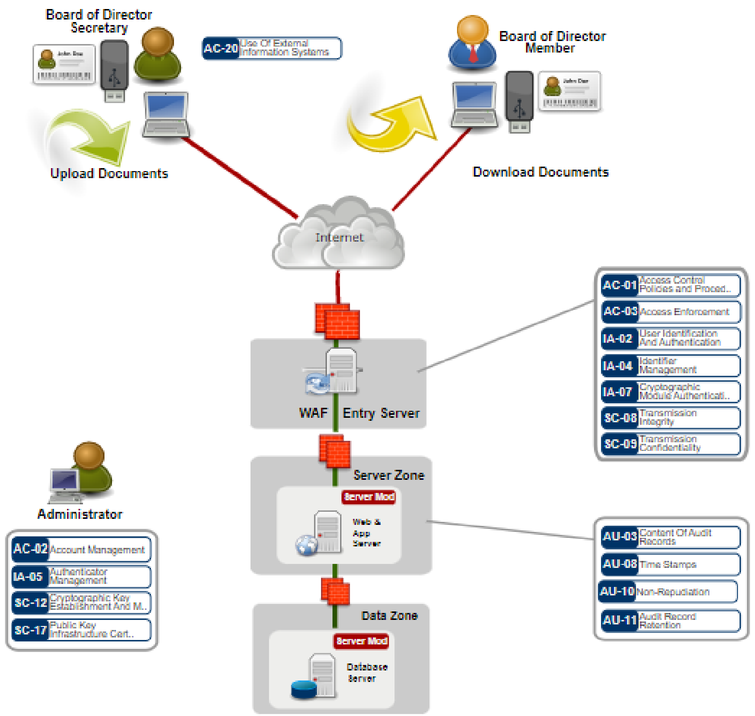
“A Data Classification scheme is often used to help understand which controls are needed for the data types processed by the organization. This scheme will be defined based on the legal, regulatory and business requirements that the organization must adhere. Common schemes used have 3 or 4 levels, including Public/Unclassified (e.g. Marketing materials), Internal Use (Information shared within the organization 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:


Board of Director Secretary
John Doe
AC-20 Use Of External Information Systems
Board of Director Member
John Doe
Upload Documents
Download Documents
Internet
AC-01 Access Control Policies and Proced..
AC-03 Access Enforcement
IA-02 User Identification And Authentication
IA-04 Identifier Management
IA-07 Cryptographic Module Authenticati..
SC-08 Transmission Integrity
SC-09 Transmission Confidentiality
WAF
Entry Server
Administrator
AC-02 Account Management
IA-05 Authenticator Management
SC-12 Cryptographic Key Establishment And M..
SC-17 Public Key Infrastructure Cert..
Server Zone
Server Mod
Web & App Server
AU-03 Content Of Audit Records
AU-08 Time Stamps
AU-10 Non-Repudiation
AU-11 Audit Record Retention
Data Zone
Server Mod
Database Server

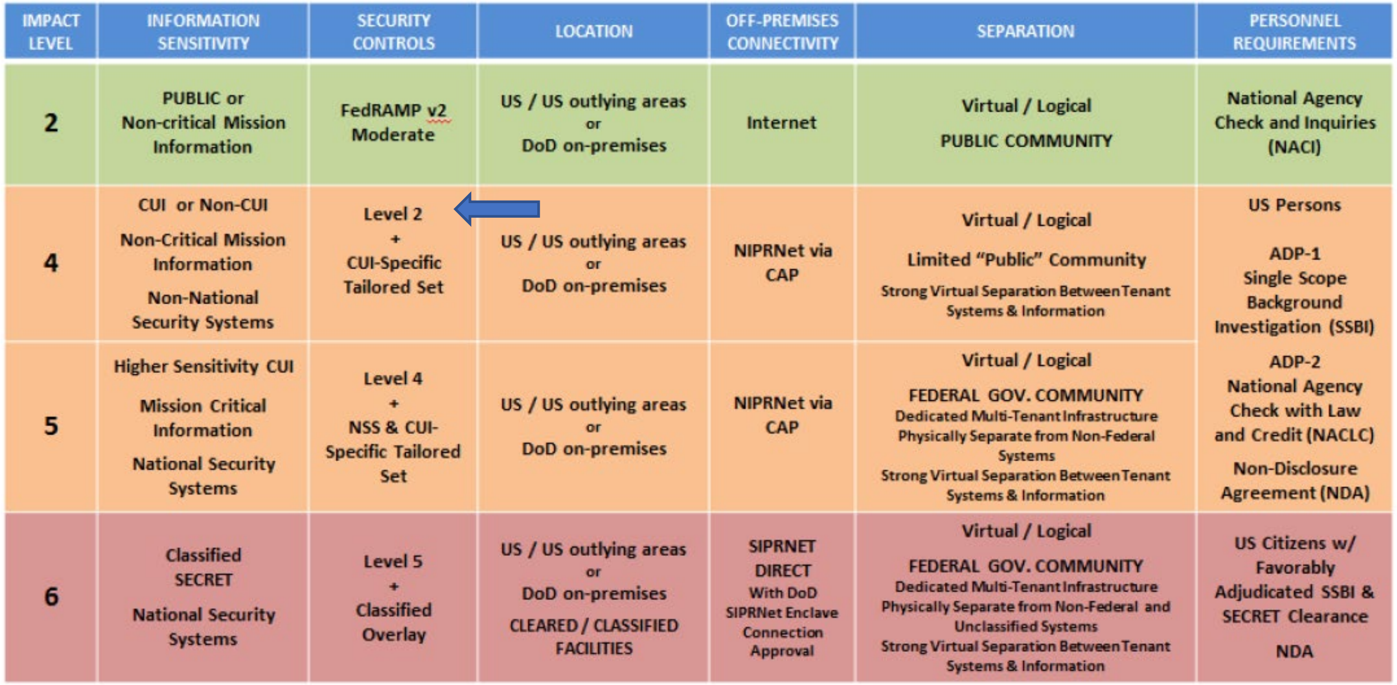
"**Synopsis**: Board of Directors Room for <u>reading highly confidential documents on an un-trusted computer</u>.

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

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

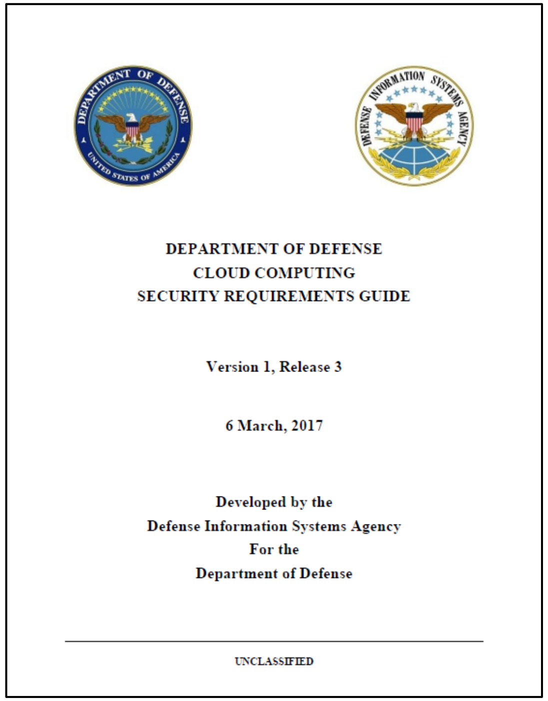
Scenario 3: Outsourced (Cloud) Networking

- 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 <u>IIL 4</u> or above!!



DEPARTMENT OF DEFENSE
CLOUD COMPUTING
SECURITY REQUIREMENTS GUIDE

Version 1, Release 3

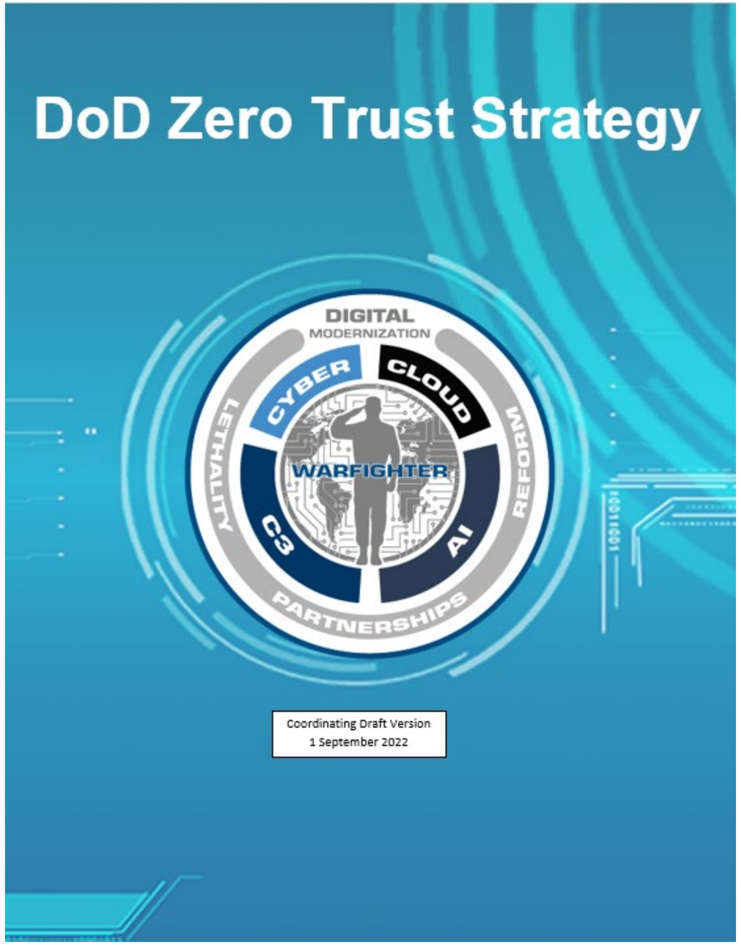
6 March, 2017

Developed by the
Defense Information Systems Agency
For the
Department of Defense

UNCLASSIFIED

New Slides on Zero Trust

Reference Documents



DoD Zero Trust Strategy

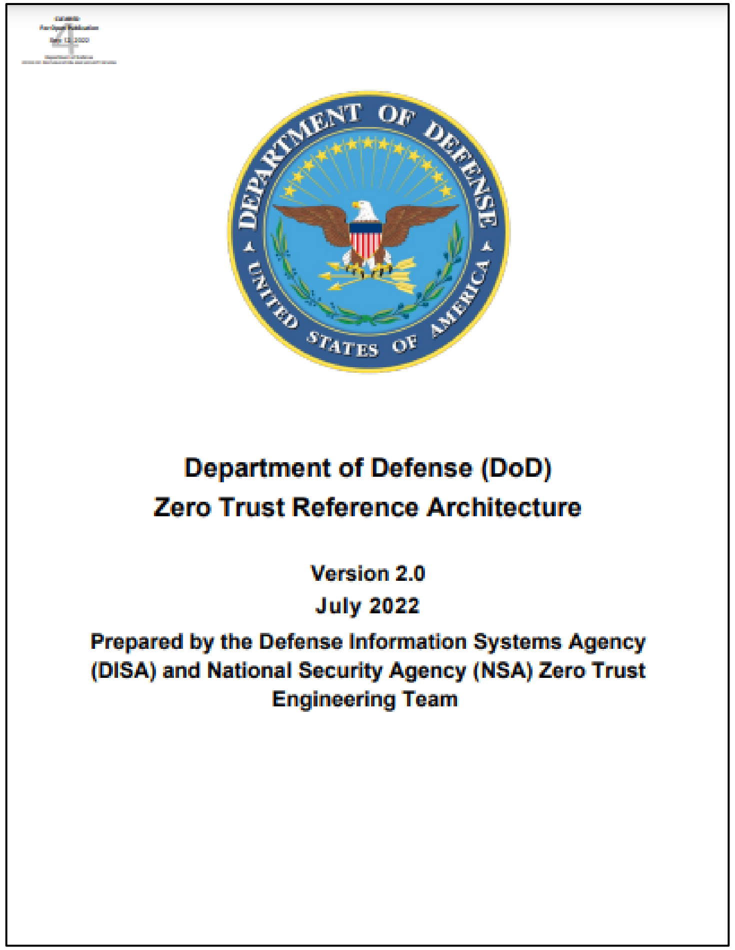
Coordinating Draft Version
1 September 2022

UNCLASSIFIED
Pre-Decisional

DoD Zero Trust Capability Execution Roadmap (COA 1)

12 July 2022

Pre-Decisional
UNCLASSIFIED



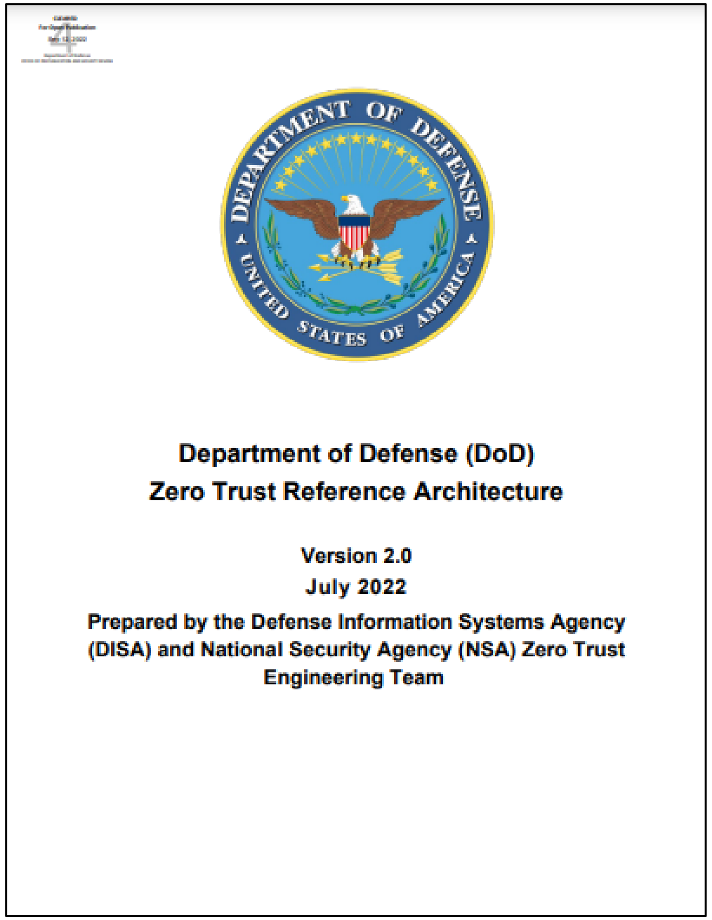
Department of Defense (DoD)
Zero Trust Reference Architecture

Version 2.0
July 2022
Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

Note: The DoD CIO (Mr. Sherman) may be publicly releasing the DoD Zero Trust Strategy – this week or next week

The DoD Zero Trust Reference Architecture is Publicly Available

DoD Zero Trust Reference Architecture



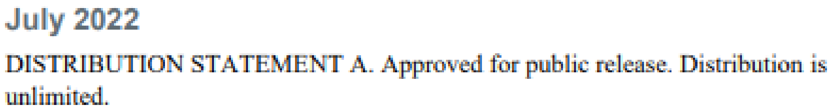
Department of Defense (DoD)
Zero Trust Reference Architecture

Version 2.0
July 2022

Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

Available at:
https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

Top of first page in the document

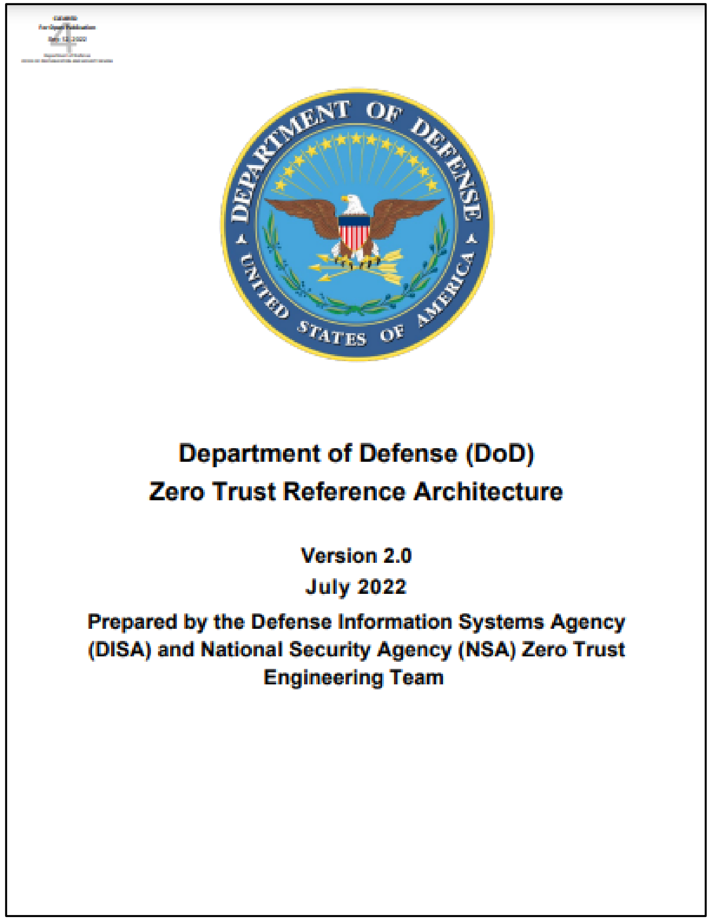


July 2022

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

"Zero Trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the Internet) or based on asset ownership (enterprise or personally owned)." (p. 9)

DoD Zero Trust Reference Architecture



Department of Defense (DoD)
Zero Trust Reference Architecture

Version 2.0
July 2022

Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

Top of first page in the document

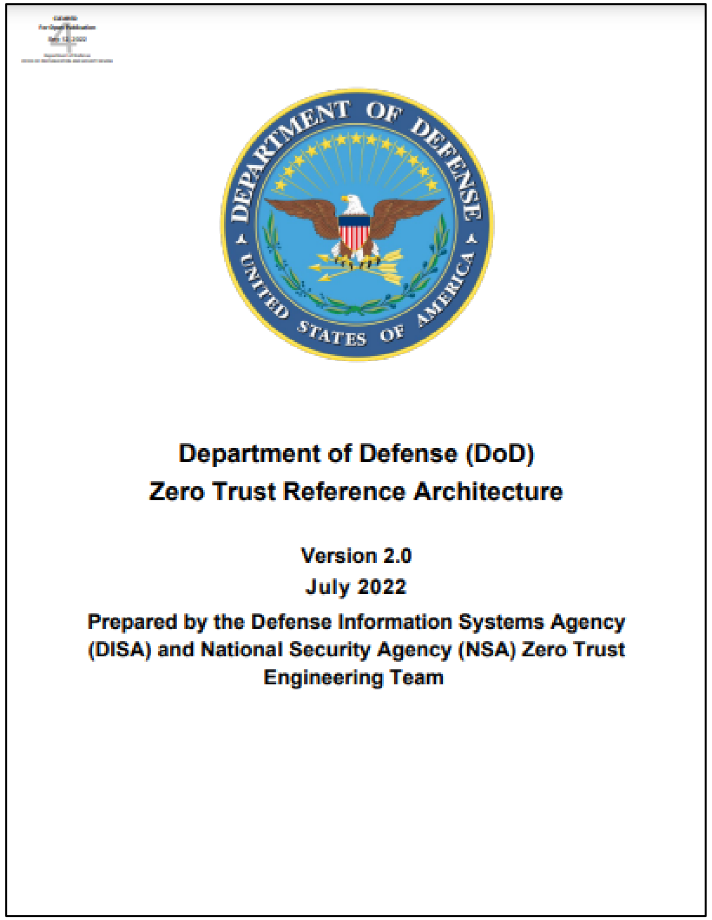
July 2022

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

"State-funded hackers are well trained, well-resourced, and persistent. The use of new tactics, techniques, and procedures combined with more invasive malware can enable motivated malicious personas to move with previously unseen speed and accuracy. Any new security capability must be resilient to evolving threats and effectively reduce threat vectors, internal and external." (p. 14)

Available at:
https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

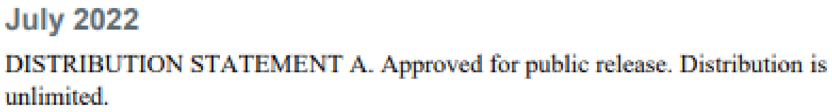
DoD Zero Trust Reference Architecture



Department of Defense (DoD)
Zero Trust Reference Architecture

Version 2.0
July 2022
Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

Top of first page in the document



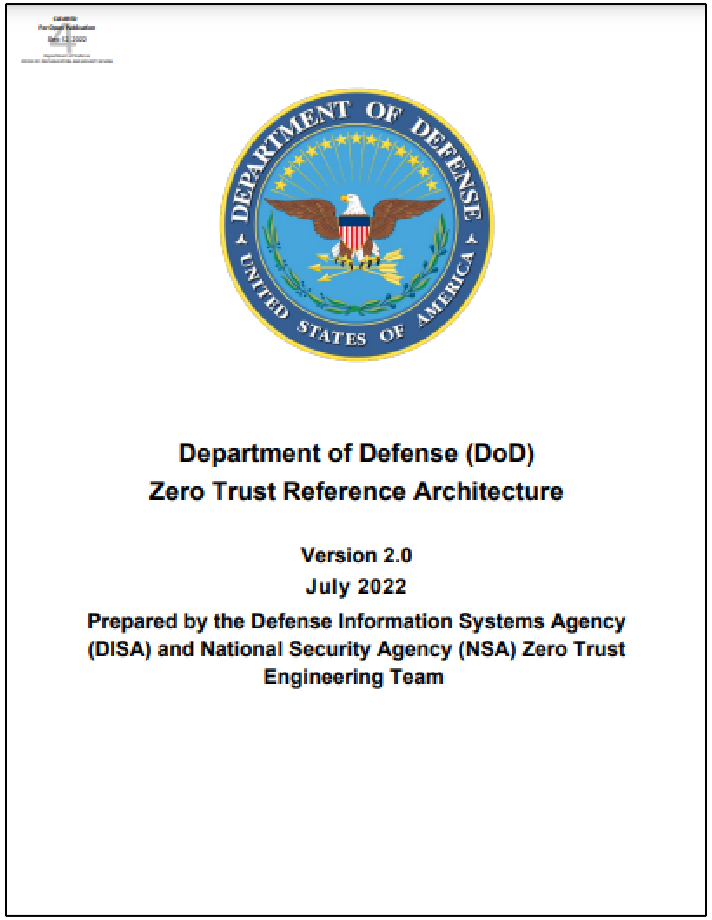
July 2022

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

“Traditional approaches to cybersecurity architectures, such as defense in depth, have resulted in complicated and redundant capabilities across the DoDIN. The prevalence of teleworking and adoption of cloud computing have caused a crossing of DoD data into new platforms; often hosted in industry and user environments. This change in the digital experience introduces new security challenges but also opportunities for leveraging important technology evolutions and ZT principals to revolutionize cyber defense.” (p. 16)

Available at:
https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

DoD Zero Trust Reference Architecture



Department of Defense (DoD)
Zero Trust Reference Architecture

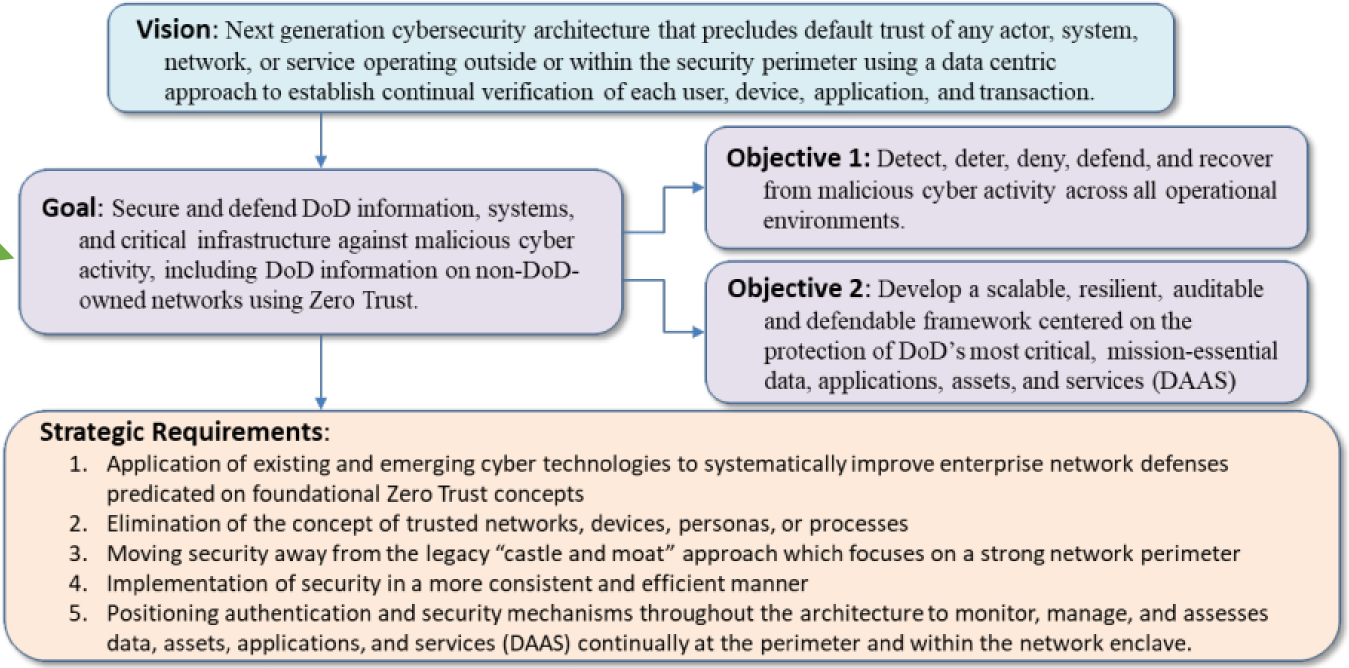
Version 2.0
July 2022
Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

Top of first page in the document

July 2022

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

Note: "on non-DoD Owned networks"



Vision: Next generation cybersecurity architecture that precludes default trust of any actor, system, network, or service operating outside or within the security perimeter using a data centric approach to establish continual verification of each user, device, application, and transaction.

Goal: Secure and defend DoD information, systems, and critical infrastructure against malicious cyber activity, including DoD information on non-DoD-owned networks using Zero Trust.

Objective 1: Detect, deter, deny, defend, and recover from malicious cyber activity across all operational environments.

Objective 2: Develop a scalable, resilient, auditable and defendable framework centered on the protection of DoD's most critical, mission-essential data, applications, assets, and services (DAAS)

Strategic Requirements:

1. Application of existing and emerging cyber technologies to systematically improve enterprise network defenses predicated on foundational Zero Trust concepts
2. Elimination of the concept of trusted networks, devices, personas, or processes
3. Moving security away from the legacy "castle and moat" approach which focuses on a strong network perimeter
4. Implementation of security in a more consistent and efficient manner
5. Positioning authentication and security mechanisms throughout the architecture to monitor, manage, and assesses data, assets, applications, and services (DAAS) continually at the perimeter and within the network enclave.

Figure 2 Zero Trust Vision (CV-1)[4]

(p. 13)

Available at:
https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

Zero Trust (ZT) Challenges

- ZT is a newer concept - difficult for organizations to develop coherent requirements & policies
- No single solution to developing ZT or single set of tools/services
- Data - not a common, open standard to interact & exchange information - can lead vendor lock due to interoperability issues
- Developing criteria/weights/threshold values requires planning & testing – requires “tuning” in implementation
- Requires detailed knowledge of assets (physical and virtual), users (including user privileges), & business processes

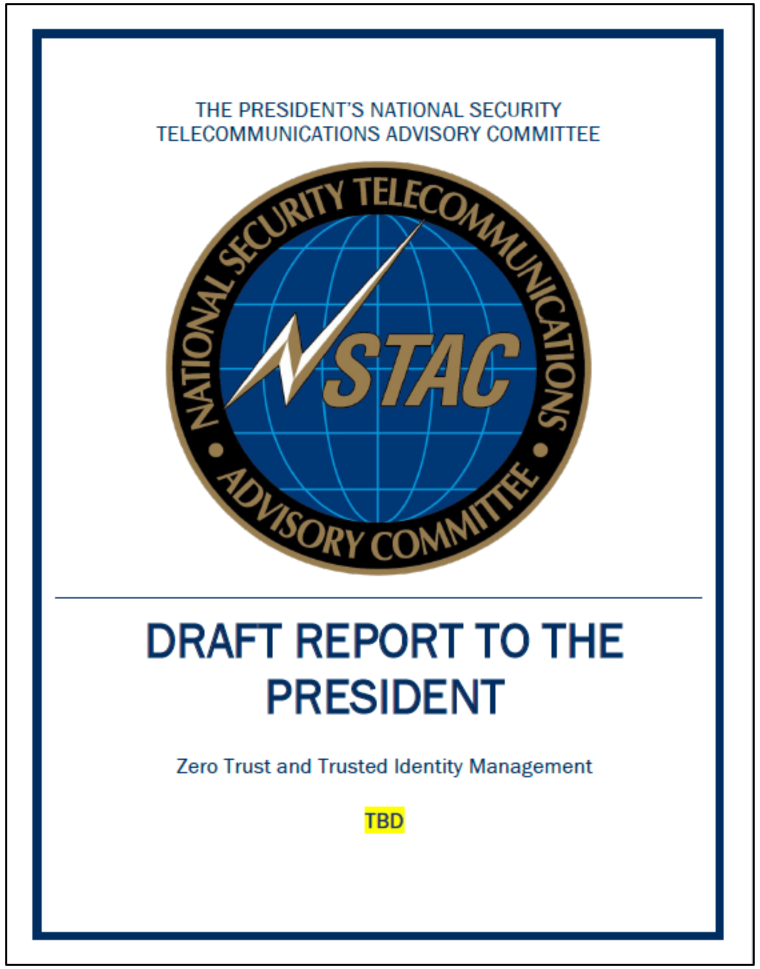
ZT Challenges

Network Security Implementation Issues:

- Changing landscape including:
  - Changing perimeter – no longer a fixed with trusted internal segments
  - Virtualized HW/SW
  - Past network protocols not secure-by-design
  - IP Address challenge – IP addresses lack any type of user knowledge to validate device trust & lack context, provide connectivity, but does not validate trust of endpoint or user

- Implementing integrated controls - visibility and transparency of network connections is problematic in implementation of networks & cybersecurity tools. Usually, integration of controls by gathering data in a Security Information & Event Management (SIEM) tools for analysis.

ZT Application



THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

DRAFT REPORT TO THE PRESIDENT

Zero Trust and Trusted Identity Management

TBD

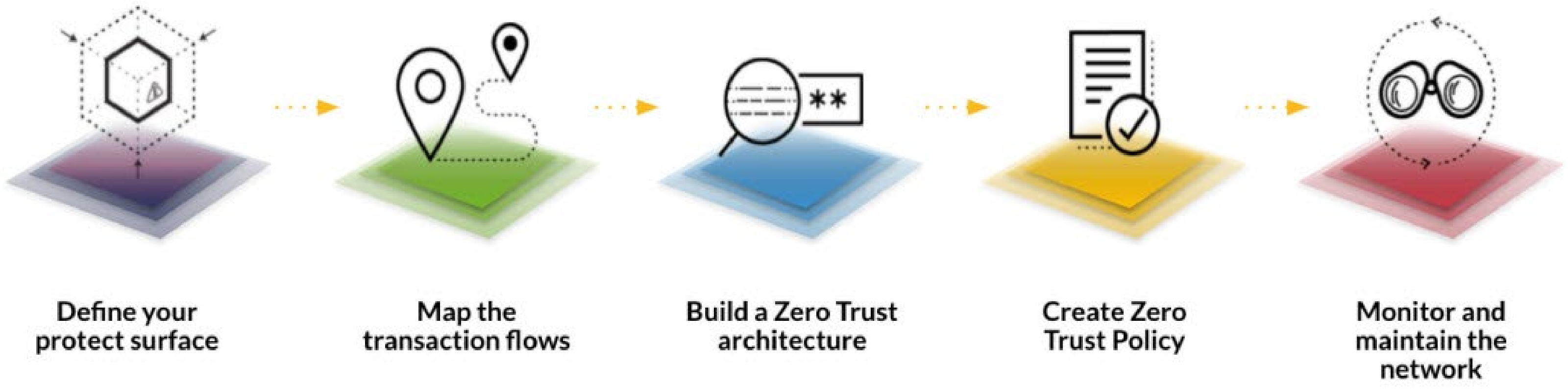
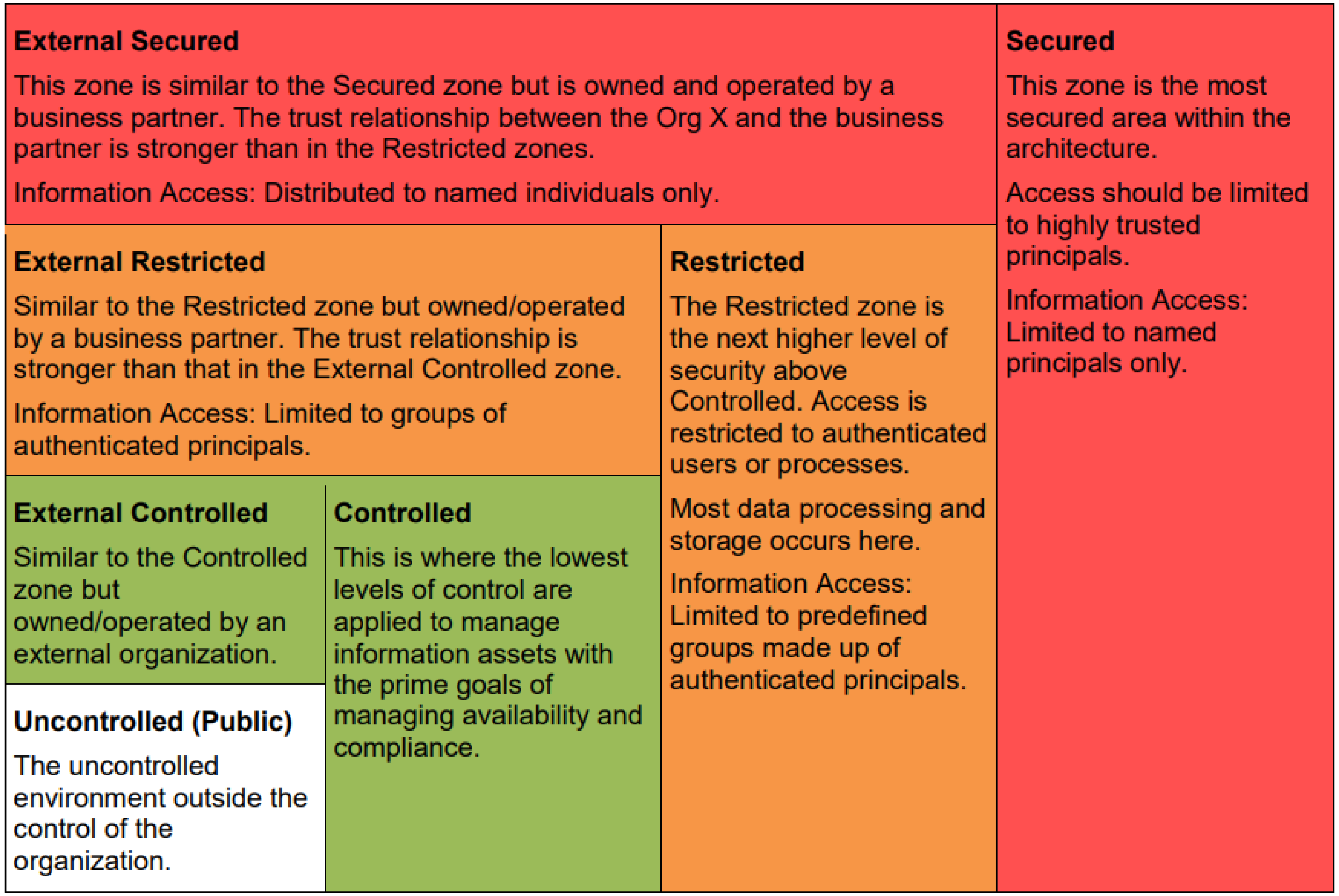

Define your protect surface
Map the transaction flows
Build a Zero Trust architecture
Create Zero Trust Policy
Monitor and maintain the network

Figure 1: Five-Step Process for Zero Trust Implementation[30]

(p. 7)

Available at: https://www.cisa.gov/sites/default/files/publications/Final%20Draft%20NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf

Data Levels of Trust



External Secured

This zone is similar to the Secured zone but is owned and operated by a business partner. The trust relationship between the Org X and the business partner is stronger than in the Restricted zones.

Information Access: Distributed to named individuals only.

Secured

This zone is the most secured area within the architecture.

Access should be limited to highly trusted principals.

Information Access: Limited to named principals only.

External Restricted

Similar to the Restricted zone but owned/operated by a business partner. The trust relationship is stronger than that in the External Controlled zone.

Information Access: Limited to groups of authenticated principals.

Restricted

The Restricted zone is the next higher level of security above Controlled. Access is restricted to authenticated users or processes.

Most data processing and storage occurs here.

Information Access: Limited to predefined groups made up of authenticated principals.

External Controlled

Similar to the Controlled zone but owned/operated by an external organization.

Controlled

This is where the lowest levels of control are applied to manage information assets with the prime goals of managing availability and compliance.

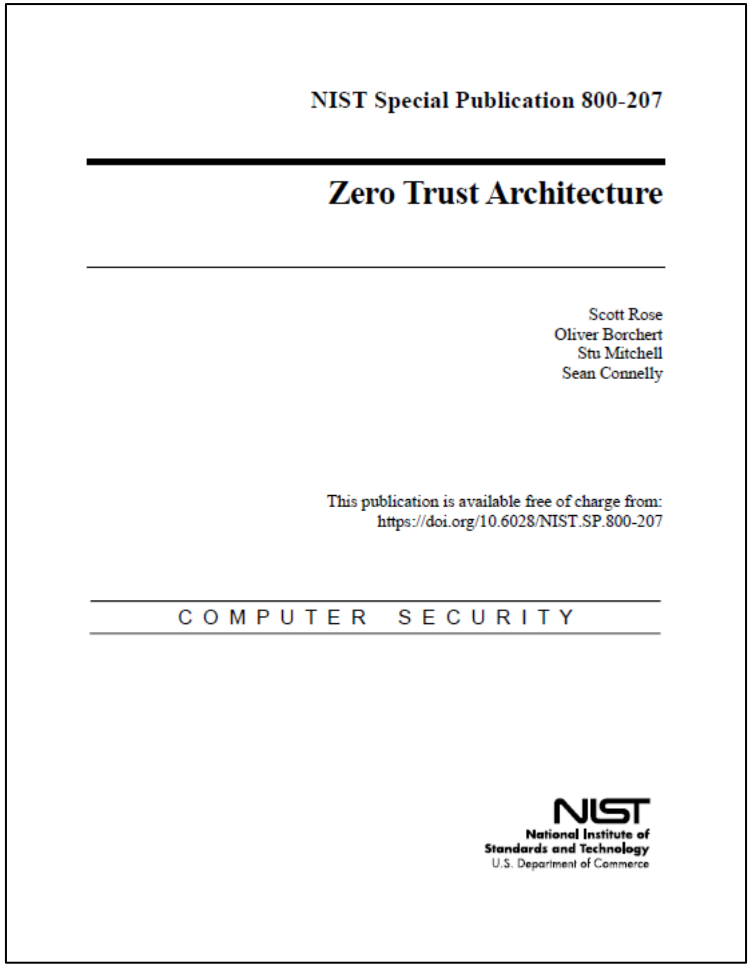
Uncontrolled (Public)

The uncontrolled environment outside the control of the organization.

Figure 11: Trust Taxonomy Model

Trust Ecosystem, The Open Group, p. 18
Available at: https://publications.opengroup.org/g141

ZTA Options



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

“3.1 Variations of Zero Trust Architecture Approaches

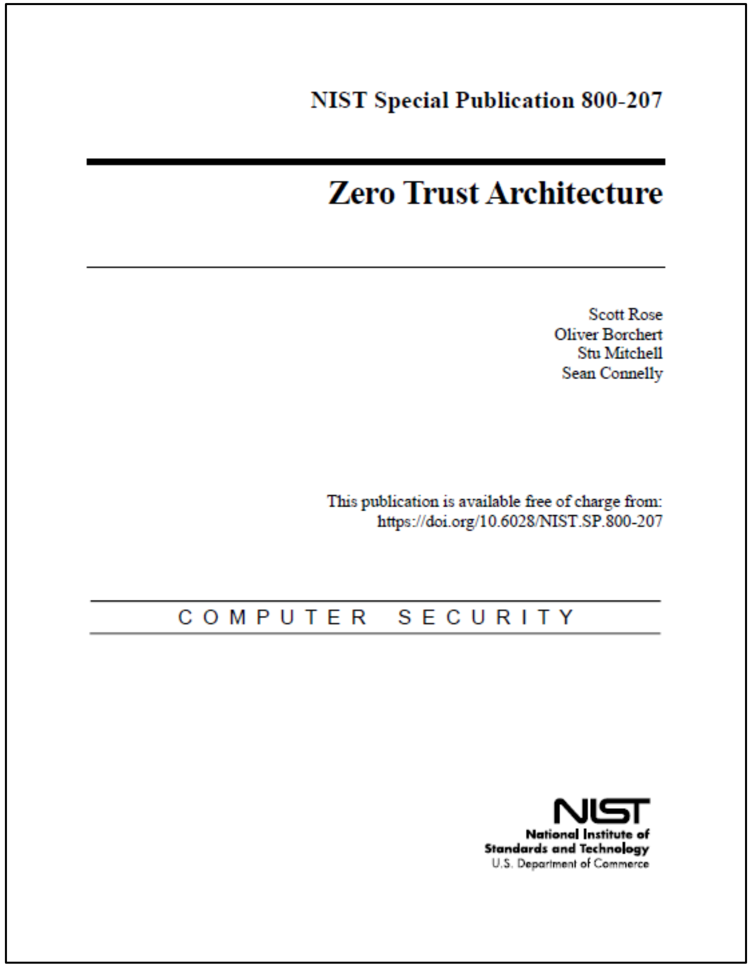
There are several ways that an enterprise can enact a ZTA for workflows. These approaches vary in the components used and in the main source of policy rules for an organization. Each approach implements all the tenets of ZT (see Section 2.1) but may use one or two (or one component) as the main driver of policies. A full ZT solution will include elements of all three approaches. The approaches include enhanced identity governance–driven, logical micro-segmentation, and network-based segmentation.

Certain approaches lend themselves to some use cases more than others. An organization looking to develop a ZTA for its enterprise may find that its chosen use case and existing policies point to one approach over others. That does not mean the other approaches would not work but rather that other approaches may be more difficult to implement and may require more fundamental changes to how the enterprise currently conducts business flows.”

p. 11

Available at:
https://csrc.nist.gov/publications/detail/sp/800-207/final

Logical Components



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

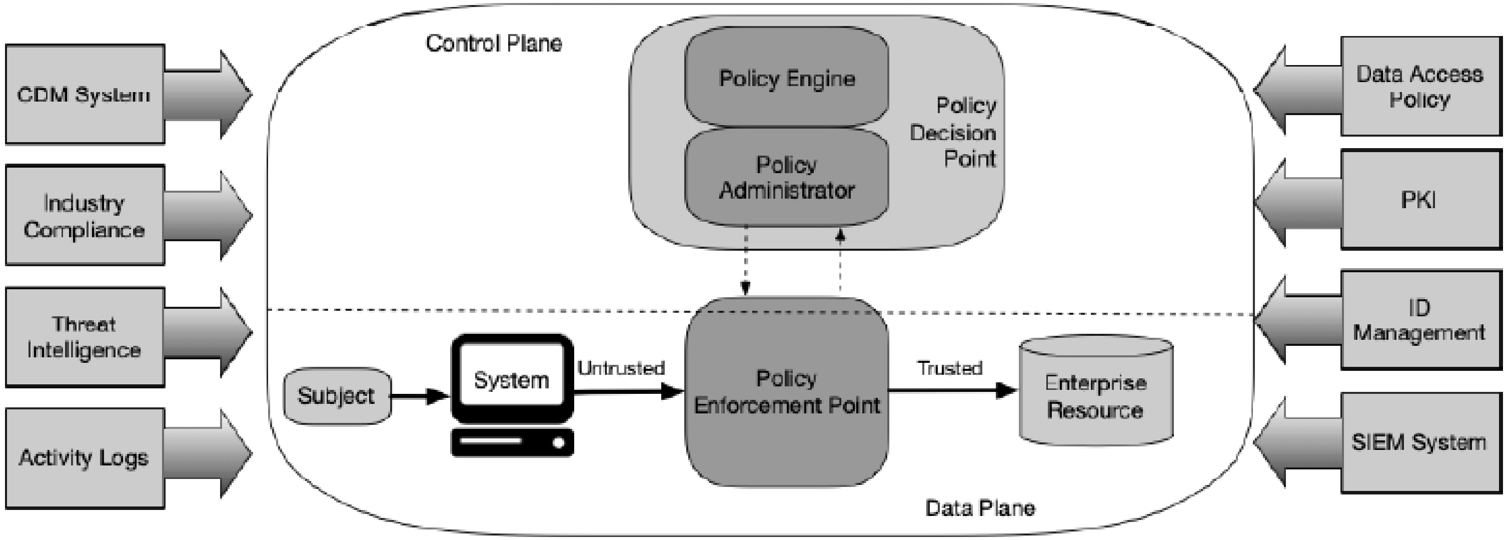
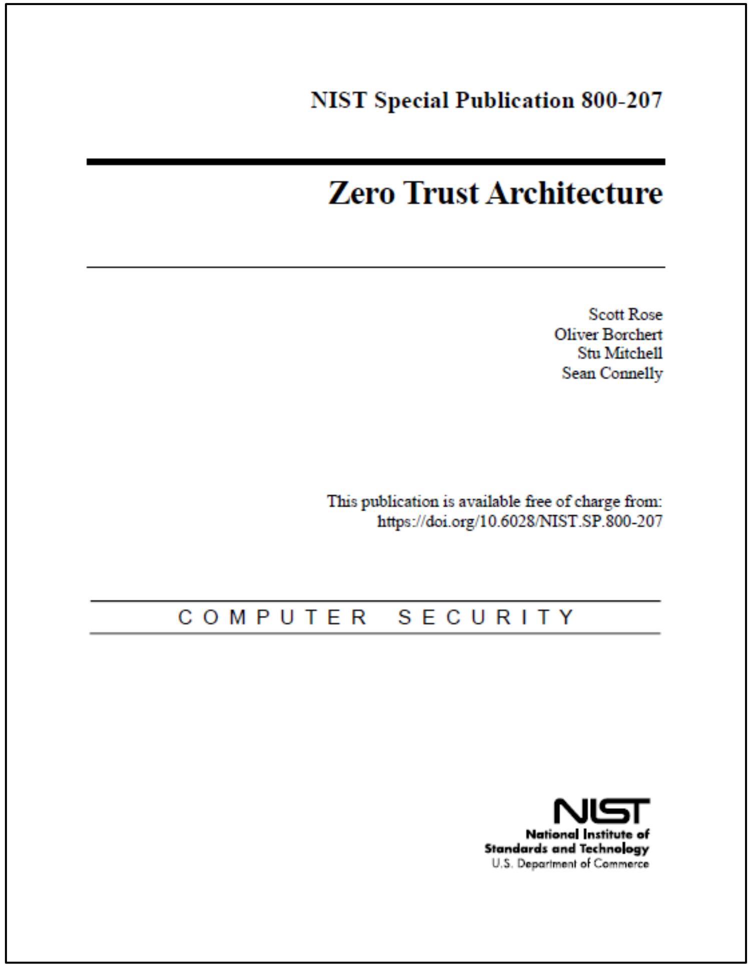


Figure 2: Core Zero Trust Logical Components

p. 9

Trust Algorithm



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

“3.3 Trust Algorithm

For an enterprise with a ZTA deployment, the policy engine can be thought of as the brain and the PE’s trust algorithm as its primary thought process. The trust algorithm (TA) is the process used by the policy engine to ultimately grant or deny access to a resource. The policy engine takes input from multiple sources (see Section 3): the policy database with observable information about subjects, subject attributes and roles, historical subject behavior patterns, threat intelligence sources, and other metadata sources. .”

p. 17

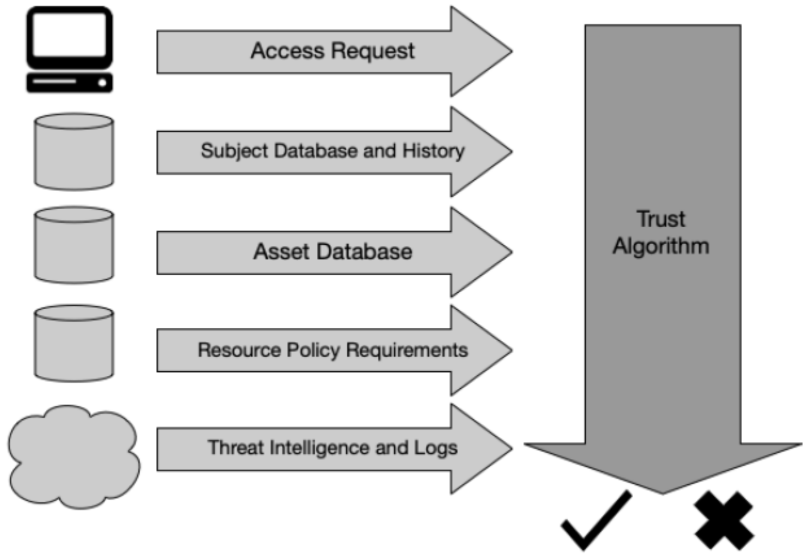

Access Request
Subject Database and History
Asset Database
Resource Policy Requirements
Threat Intelligence and Logs
Trust Algorithm

Figure 7: Trust Algorithm Input

p. 18

ZT Progression

Progression of Data for Trust Algorithm use:

- Telemetry for Access Control
- Use of Threat Intelligence & Threat Feeds
- Signals & Telemetry for Visibility & Analytics
- Signals & Telemetry for Automation & Orchestration

Use of these various types of data sources in a policy decision point within a trust algorithm is a critical concept

Key Considerations

GSA

Zero Trust Architecture (ZTA)

Buyer's Guide

GSA July 2022 Version 2.0

Available at:
https://www.gsa.gov/technology/technology-products-services/it-security/zero-trust-and-gsa

"8. Key Considerations for Products, Services, and Solutions

On some level, any security vendor could claim to provide a ZTA offering. Agencies should follow the guidance found in NIST SP 800-207, which provides systematic guidelines for updating network cybersecurity in a world where remote work is prevalent, and traditional network defenses are inadequate. In following this guidance, agencies can improve their security posture by implementing the Zero Trust principles documented in NIST SP 800-207 with optimal configurations according to their business needs.

It is important to note that although vendors have made great strides in building Zero Trust based solutions, there is no single end-to-end, comprehensive Zero Trust Network solution. Additionally, agencies should realize it is not necessary to rip and replace existing cybersecurity tools, but rather take small incremental steps in deploying ZTA tools on top of existing infrastructure. In developing a ZTA implementation strategy for essential Zero Trust offerings such as identity and access management, encryption, multifactor authentication, and next generation firewalls, agencies should consider General Services Administration (GSA) Offered Products, Services, and Solutions for a ZTA."

p. 4 - 5

Misrepresentation

How cybersecurity vendors are misrepresenting zero trust

https://venturebeat.com/security/how-cybersecurity-vendors-are-misrepresenting-zero-trust/

“The zero-trust vision that cybersecurity vendors are selling isn’t the reality enterprises are experiencing. The disconnect begins during initial sales cycles, where the promises of ease of use, streamlined API integration and responsive service lead to enterprises buying solutions that don’t work. Unfortunately, enterprises are getting more challenges than the vision vendors sold.

“Vendors have a well-meaning, but bad habit, of trying to frame whatever they’ve been selling for years as ‘zero trust,’” said David Holmes, senior analyst at Forrester. “We’ve seen this time and again. In reality, there are precious few ZT-specific technologies: zero-trust network access (ZTNA), microsegmentation and PIM/PAM [privileged identity management/privileged access management]. Many other techs, like identity and access management [IAM], network automation and endpoint encryption can be used *in support* of zero trust, but they aren’t ZT, by themselves. A good rule of thumb is that if the vendor didn’t design the product to be ZT, it isn’t.” ”

Questions