



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**

July 2022

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

Document Prepared By	Date
Name: Robert Freter DISA Zero Trust Program Lead (ID2)	June 2022

1	PURPOSE AND STRATEGIC GOALS	9
1.1	Introduction	9
1.2	Purpose	9
1.3	Scope	10
1.3.1	Stakeholders	10
1.3.2	Organization of the Reference Architecture	10
1.3.3	Timeframe	12
1.4	Vision and Goals (CV-1)	13
1.4.1	Vision and High-Level Goals (CV-1)	14
1.4.2	Zero Trust Strategy	15
1.5	Cybersecurity (Transition) Problem Statement (OV-1)	16
1.6	Overall Target Environment (OV-1)	18
1.7	Assumptions	19
1.8	Constraints	20
2	PILLARS AND PRINCIPLES	20
2.1	Overview	20
2.2	Concept and Tenets of Zero Trust	20
2.3	Pillars	21
2.4	Reference Architecture Principles (OV-6a)	23
3	CAPABILITIES	25
3.1	Capabilities Taxonomy (CV-2)	25
3.2	FFP: Pillars, Resources & Capability Mapping	31
4	USE CASES	35
4.1	Data Centric Security Protections (OV-1)	35
4.2	Data-Centric Security Protections (OV-2)	37
4.3	Data Encryption Protections (OV-2)	39
4.4	Coordinating Policy for Data-Centric Security Protections (OV-2)	41

4.5	Data Analytics & AI (OV-1).....	42
4.6	Data Analytics & AI (SV-1).....	44
4.7	Centralized Orchestration & Policy Management (OV-1).....	45
4.8	Centralized Orchestration & Policy Management (OV-2).....	46
4.9	Dynamic, Adaptive Policy Feedback Loop (OV-1).....	47
4.10	VPN-Less Implementation (OV-1)	48
4.11	East-West Segmentation (OV-1)	49
4.12	Global Uniform Device Hygiene (OV-1)	50
4.13	Global Uniform Device Hygiene (OV-2)	52
4.14	Dynamic, Continuous Authentication (OV-1).....	54
4.15	Dynamic, Continuous Authentication (OV-2).....	56
4.16	Conditional Authorization (OV-1).....	60
4.17	Conditional Authorization (OV-2).....	62
5	TECHNICAL POSITIONS	63
5.1	Emerging Technologies.....	63
5.2	Standards, Associated Architectures and Guides	64
5.3	Linkages to Other Architectures.....	65
5.3.1	DoD Cybersecurity Reference Architecture (CS RA) Integration	65
5.3.2	DoD ICAM Reference Design (RD).....	66
5.3.3	NIST Special Publication 800-207 Zero Trust Architecture	67
6	SECURITY ASSESSMENT	68
6.1	Governance	68
6.2	Data Governance (OV-2)	68
6.3	Securing Supply Chain (OV-2)	70
7	ARCHITECTURE PATTERNS.....	71
7.1	Architecture Patterns (CV-4)	71
7.1.1	Domain Policy Enforcement for Resource Access (SV-1).....	72
7.1.2	Software Defined Perimeter (OV-2)	73

7.1.3 ZT Broker Integration (SV-1).....	74
7.1.4 Micro Segmentation (SV-1).....	74
7.1.5 Macro Segmentation (SV-1).....	78
7.2 External Services	78
7.2.1 SvcV-1: External Services(SvcV-1).....	79
7.2.2 SvcV-2: Enterprise Federated Identity Service (SvcV-2)	80
8 TRANSITION ARCHITECTURE PLANNING (FFP).....	81
8.1 Maturity Model (FFP).....	81
8.2 Baseline (OV-1).....	82
8.3 Transition (OV-1)	83
9 APPENDIX (AV-2)	84
9.1 Systems	85
9.2 Services	90
9.3 General Terms	92
9.4 DIV-1	93
9.5 StdV-1-2 References	96
9.6 Capability Table.....	97
10 REFERENCES	104