Zscaler GovCloud Services for CMMC

Feature Applicability To Cybersecurity Maturity Model Certification

4/21/2021

zscaler™

Table of Contents

Executive Summary

Zscaler, along with consulting support from RPO, Landers and Company, reviewed the Zscaler Zero Trust Exchange for its applicability within the Cybersecurity Maturity Capability Model (CMMC) framework. The Zero Trust Exchange is Zscaler's cloud-delivered security environment comprised of the Zscaler Internet Access-Government (ZIA GOV) and the Zscaler Private Access-Government (ZPA GOV) systems. The findings below provide an overview of Zscaler capabilities, functions, and features that will empower an organization to modernize their security architecture, while also meeting critical CMMC controls across all levels.

It was found that Zscaler can enable an organization to support or meet 82 controls by modernizing how the organization performs transport security. In addition, 43 of the remaining controls are policy/process adoption and Zscaler services, leaving only a handful out of scope. Leveraging the Zscaler Zero Trust Exchange greatly lowers the amount of effort an organization would endure for CMMC accreditation.

Finally, a modern SASE solution that is constructed in software-defined perimeter principles and designed to be a foundational building block for a Zero Trust Architecture will minimize ongoing maintenance. A common control plane with unified administrative and analysis panels reduces the time to complete a 3PAO audit, and allows for common policies throughout the organization.

The Case for CMMC

CMMC is the new set of cybersecurity standards developed by the Department of Defense (DoD) to protect defense contractors from cyber-attacks. As a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB), CMMC will be a required certification for every organization that bids on a DOD contract. The rollout is expected to be phased over the next five years, at which point all DOD contracts will require CMMC certification – impacting roughly 300,000 companies and over $400B of DOD contract awards annually. The aggregate loss of controlled unclassified information (CUI) from the Defense Industrial Base (DIB) increases risk to national economic security and in turn, national security. In order to reduce this risk, the DIB must enhance its protection of CUI in its networks.

Additionally, DFARS Clause 252.204-7012 and NIST 800-171 cybersecurity requirements for prime and subcontractors are no longer voluntary. DoD audits, coupled with the Cybersecurity Maturity Model Certification (CMMC) will require all companies conducting business with the DoD to be certified by a third party, or C3PAO.

A C3PAO is a service provider organization that the CMMC Accreditation Body (CMMC-AB) has accredited and authorized to conduct CMMC assessments. The C3PAO also submits findings and recommendations to the CMMC-AB in order to certify that Organizations Seeking Certification (OSCs) comply with the CMMC maturity level (1 through 5) to perform in a given A&D contract.

Zscaler GovCloud: Crossroads of Transformation and CMMC Compliance

The Zscaler GovCloud enables organizations to securely connect users to the internet and applications, regardless of device, location, or network, improving security while reducing cost and complexity while delivering a better user experience.

As government agencies implement IT modernization initiatives, they need to reduce appliance complexity and improve user experience. ZIA GOV enables agencies to route mission-critical traffic straight to the cloud, without the latency of hair pinning through security appliances within the legacy perimeter architecture. ZIA GOV is the first secure internet and web gateway solution to meet the guidance of the TIC 3.0 initiative.

Additionally, ZPA GOV securely connects trusted users to trusted internal applications, without placing users on the network. ZPA GOV eliminates the need for traditional, on-premises, VPN appliances that create high operational overhead and compromise security, cost, and user experience.

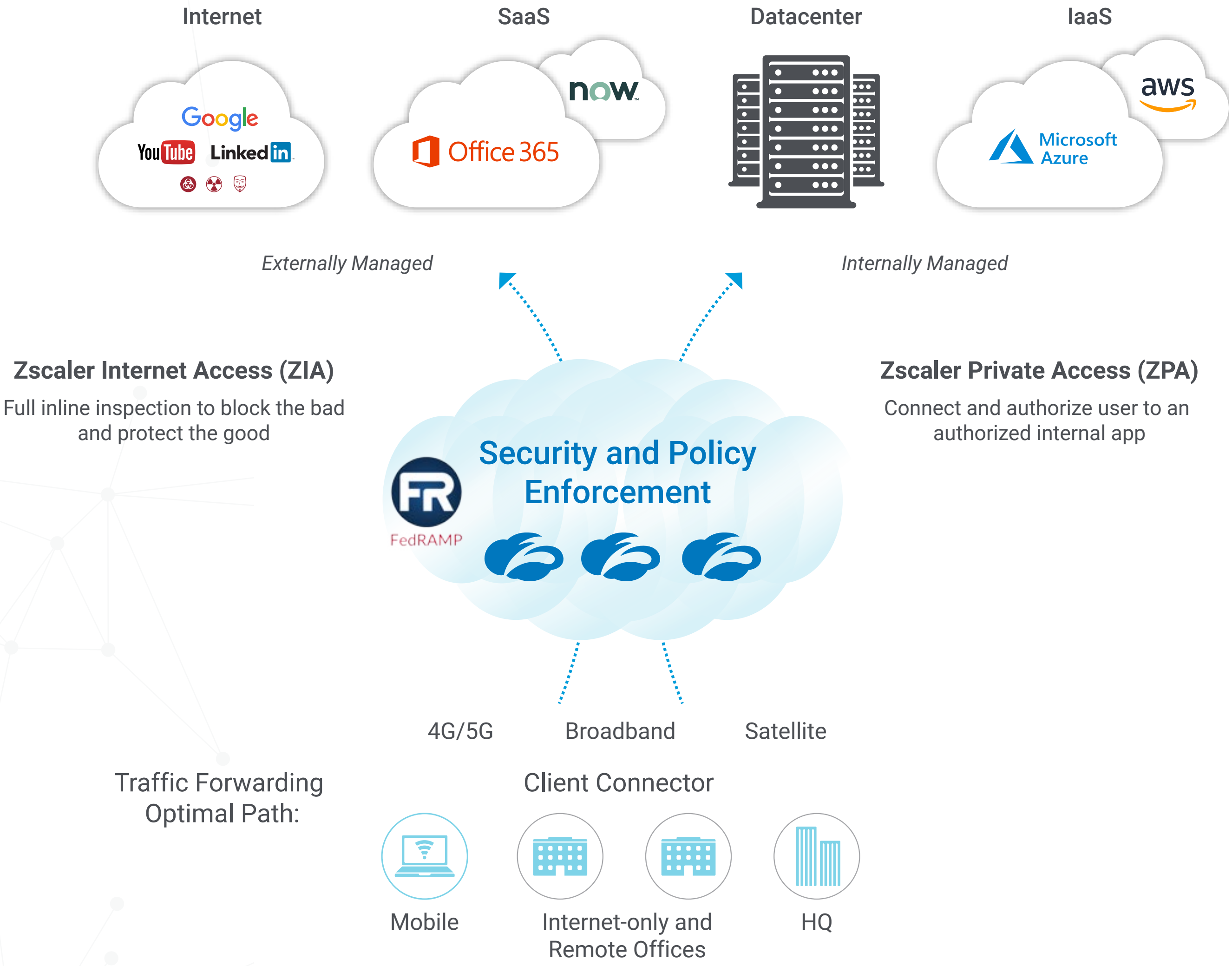

Internet
SaaS
Datacenter
IaaS
Google
YouTube
LinkedIn
now
Office 365
aws
Microsoft Azure
Externally Managed
Internally Managed
Zscaler Internet Access (ZIA)
Full inline inspection to block the bad and protect the good
Zscaler Private Access (ZPA)
Connect and authorize user to an authorized internal app
Security and Policy Enforcement
FR
FedRAMP
4G/5G
Broadband
Satellite
Traffic Forwarding Optimal Path:
Client Connector
Mobile
Internet-only and Remote Offices
HQ

Figure 1 – The Zscaler Zero Trust Exchange

Leveraging FedRAMP High Impact Certification

Zscaler achieved its first win with ZIA in 2019, becoming the first cloud-based secure web gateway solution to earn FedRAMP certification. In 2020, ZPA achieved a FedRAMP JAB High authorization. A JAB High Baseline authorization for ZIA is a significant step forward, enabling Zscaler to offer more comprehensive solutions in the government marketplace, including Advanced Cloud Sandbox, Zscaler Digital Experience (ZDX), and Zscaler Cloud Connector.

In 2020, Gartner recognized Zscaler as the only leader in its December 2020 Magic Quadrant for Secure Web Gateways, underscoring the Zscaler Zero Trust Exchange and Zscaler Advanced Cloud Sandbox as the industry model for the successful implementation of the Cybersecurity and Infrastructure Security Agency's (CISA's) Trusted Internet Connection (TIC) 3.0 guidelines. Zscaler is committed to helping keep civilian agencies and employees safe, productive, and focused on their mission.

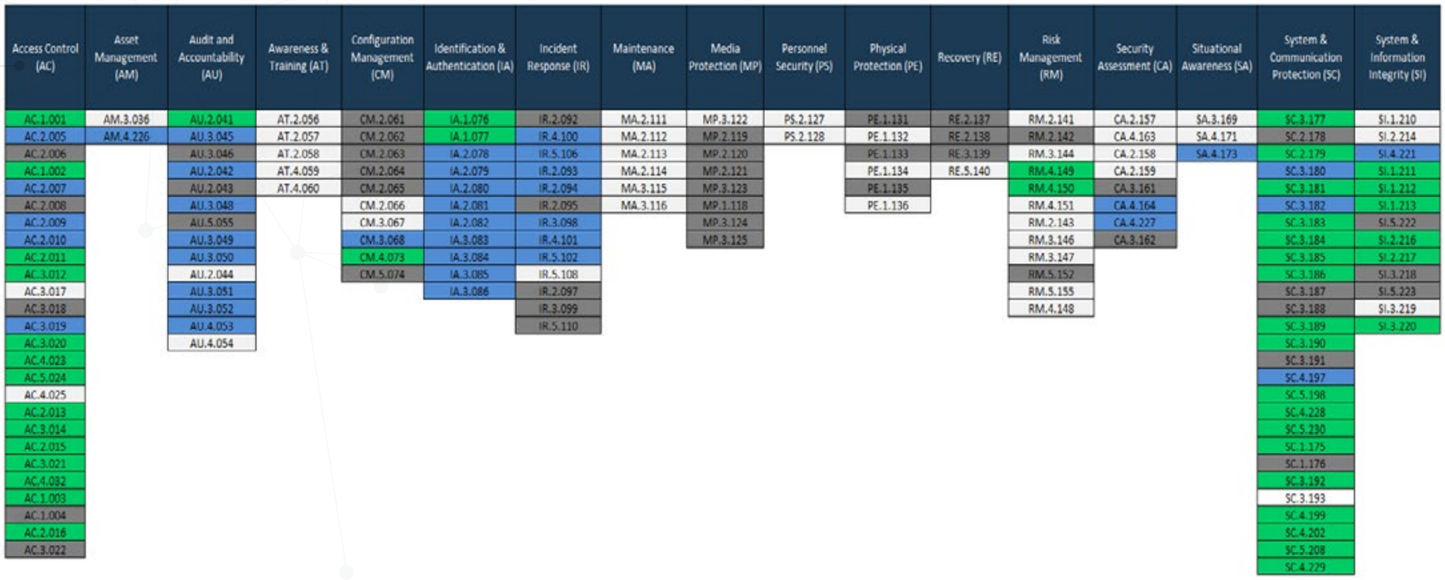
In February 2021, the FedRAMP Connect program announced that Zscaler Internet Access (ZIA) is prioritized for Joint Authorization Board (JAB) FedRAMP certification at the High Impact Level. ZIA, combined with Zscaler Private Access (JAB authorized at the High Impact Level) are the core of the Zscaler Zero Trust Exchange.

The JAB selects an extremely limited number of providers for review each year – the primary criteria is government-wide demand for the solution. Additionally, in order to be prioritized for the JAB High Impact Level, systems must comply with 421 controls by automating as many processes as possible, including the capability to provide ongoing continuous monitoring to support authorization and reauthorization decisions. Zscaler's selection highlights the value currently being delivered to 100+ federal agencies, Federal Systems Integrators (FSIs), and partners. Over one million total users are currently supported in Zscaler GovCloud; and there is widespread interest in Zscaler solutions across the federal government.

Certification at the High Impact level has positioned Zscaler uniquely to support more customers in the Department of Defense (DoD) and Intelligence Community (IC) organizations as well. With sponsorship to the data impact Levels (IL) 4 and 5, the Zscaler solution will be used to protect the government's most sensitive, unclassified data wherever it is maintained supporting their multi-hybrid cloud strategy. This includes data where loss of confidentiality, integrity, or availability may have a catastrophic effect on operations, assets, or individuals.

Mapping CMMC Controls to the Zscaler GovCloud

🟩 MAPS TO CMMC CONTROL 🟦 SUPPORTS CMMC CONTROL ⬜ N/A – CUSTOMER PROCESS ⬛ N/A



Access Control (AC)	Asset Management (AM)	Audit and Accountability (AU)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Recovery (RE)	Risk Management (RM)	Security Assessment (CA)	Situational Awareness (SA)	System & Communication Protection (SC)	System & Information Integrity (SI)
🟩 AC.1.001	⬜ AM.3.036	🟩 AU.2.041	⬜ AT.2.056	⬛ CM.2.061	🟩 IA.1.076	⬛ IR.2.092	⬜ MA.2.111	⬜ MP.3.122	⬜ PS.2.127	⬛ PE.1.131	⬛ RE.2.137	⬜ RM.2.141	⬜ CA.2.157	⬜ SA.3.169	🟩 SC.3.177	⬜ SI.1.210
🟦 AC.2.005	🟦 AM.4.226	🟦 AU.3.045	⬜ AT.2.057	⬛ CM.2.062	🟩 IA.1.077	🟦 IR.4.100	⬜ MA.2.112	⬛ MP.2.119	⬜ PS.2.128	⬜ PE.1.132	⬛ RE.2.138	⬛ RM.2.142	⬜ CA.4.163	⬜ SA.4.171	⬛ SC.2.178	⬜ SI.2.214
⬛ AC.2.006		⬛ AU.3.046	⬜ AT.2.058	⬛ CM.2.063	🟦 IA.2.078	🟦 IR.5.106	⬜ MA.2.113	⬛ MP.2.120		⬛ PE.1.133	⬛ RE.3.139	⬜ RM.3.144	⬜ CA.2.158	🟦 SA.4.173	🟩 SC.2.179	🟦 SI.4.221
🟩 AC.1.002		🟦 AU.2.042	⬜ AT.4.059	⬛ CM.2.064	🟦 IA.2.079	🟦 IR.2.093	⬜ MA.2.114	⬛ MP.2.121		⬜ PE.1.134	⬜ RE.5.140	🟩 RM.4.149	⬜ CA.2.159		🟦 SC.3.180	🟩 SI.1.211
🟦 AC.2.007		⬛ AU.2.043	⬜ AT.4.060	⬛ CM.2.065	🟦 IA.2.080	🟦 IR.2.094	⬜ MA.3.115	⬛ MP.3.123		⬛ PE.1.135		🟩 RM.4.150	⬛ CA.3.161		🟩 SC.3.181	🟩 SI.1.212
⬛ AC.2.008		🟦 AU.3.048		⬜ CM.2.066	🟦 IA.2.081	⬛ IR.2.095	⬜ MA.3.116	⬛ MP.1.118		⬜ PE.1.136		⬜ RM.4.151	🟦 CA.4.164		🟦 SC.3.182	🟩 SI.1.213
🟦 AC.2.009		⬛ AU.5.055		⬜ CM.3.067	🟦 IA.2.082	🟦 IR.3.098		⬛ MP.3.124				⬜ RM.2.143	🟦 CA.4.227		🟩 SC.3.183	⬛ SI.5.222
🟦 AC.2.010		🟦 AU.3.049		🟦 CM.3.068	🟦 IA.3.083	🟦 IR.4.101		⬛ MP.3.125				⬜ RM.3.146	⬛ CA.3.162		🟩 SC.3.184	🟩 SI.2.216
🟩 AC.2.011		🟦 AU.3.050		🟩 CM.4.073	🟦 IA.3.084	🟦 IR.5.102						⬜ RM.3.147			🟩 SC.3.185	🟩 SI.2.217
🟩 AC.3.012		⬜ AU.2.044		⬛ CM.5.074	🟦 IA.3.085	⬜ IR.5.108						⬛ RM.5.152			🟩 SC.3.186	⬛ SI.3.218
⬜ AC.3.017		🟦 AU.3.051			🟦 IA.3.086	⬛ IR.2.097						⬜ RM.5.155			⬛ SC.3.187	⬛ SI.5.223
⬛ AC.3.018		🟦 AU.3.052				⬛ IR.3.099						⬜ RM.4.148			⬛ SC.3.188	⬜ SI.3.219
🟦 AC.3.019		🟦 AU.4.053				⬛ IR.5.110									🟩 SC.3.189	🟩 SI.3.220
🟩 AC.3.020		⬜ AU.4.054													🟩 SC.3.190	
🟩 AC.4.023															⬛ SC.3.191	
🟩 AC.5.024															🟦 SC.4.197	
⬜ AC.4.025															🟩 SC.5.198	
🟩 AC.2.013															🟩 SC.4.228	
🟩 AC.3.014															🟩 SC.5.230	
🟩 AC.2.015															🟩 SC.1.175	
🟩 AC.3.021															⬛ SC.1.176	
🟩 AC.4.032															🟩 SC.3.192	
🟩 AC.1.003															⬜ SC.3.193	
⬛ AC.1.004															🟩 SC.4.199	
🟩 AC.2.016															🟩 SC.4.202	
⬛ AC.3.022															🟩 SC.5.208	
															🟩 SC.4.229	

Figure 2 – CMMC Control Graph Mapped to Zscaler GovCloud Platform

As outlined in the above graph, Zscaler organized its CMMC capabilities into one of four categories:

- Maps to Requirement: Zscaler GovCloud provides a direct means to support the practice requirement presuming proper configuration and enrollment.
- Supports Requirement: Through the available features of Zscaler GovCloud, additional customer activities are facilitated, which support compliance with the practice requirement.
- Not Applicable (Customer Process): Zscaler GovCloud provides no support for the CMMC requirement due to policies and procedures that must be in place by the customer. In these instances where the CMMC practice identified is process-driven and therefore customer responsibility, Zscaler is qualified to be a trusted partner, leveraging our high-impact FedRAMP experience within the Zero Trust community.
- Not Applicable: Controls that are identified as the full responsibility of the customer and require things like physical security capabilities, media protection across environment, or data recovery just to name a few examples.

Zscaler's CMMC control count can also be described within the CMMC's five levels of maturity with 9 controls supporting or mapping for Level 1, 20 controls supporting or mapping for Level 2, 29 controls supporting or mapping for Level 3, 18 controls supporting or mapping Level 4, and 6 controls supporting or mapping for Level 5.

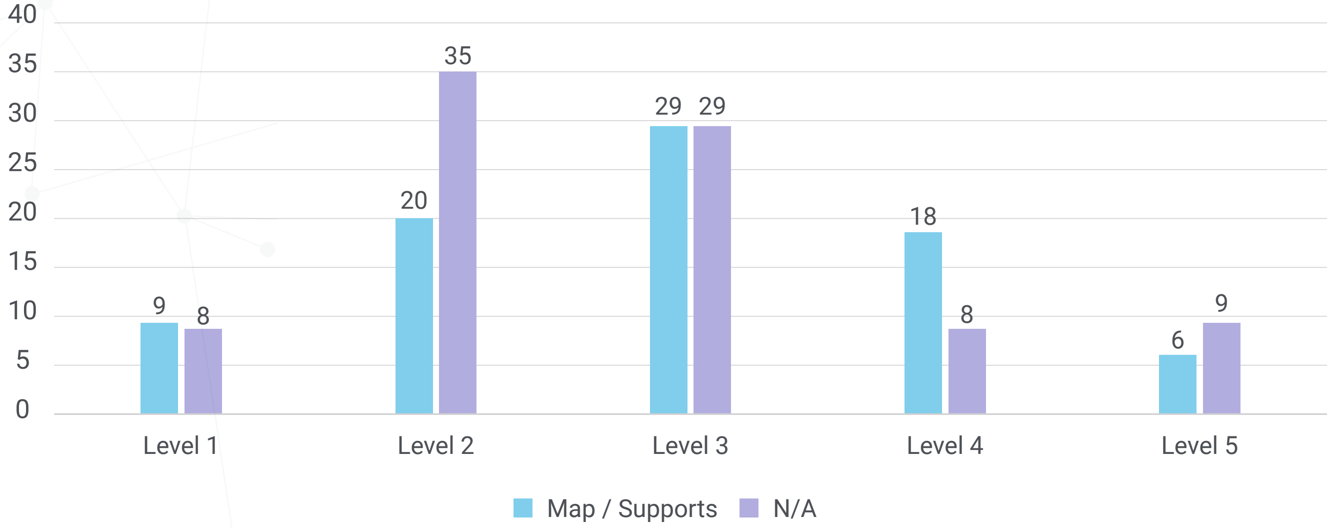


Figure 2 – CMMC Control Graph Mapped to Zscaler GovCloud Platform

Zscaler Technical Abilities across CMMC Practices

The following section highlights the technical abilities of the Zscaler GovCloud solution in how they either support or map to the required CMMC practices.

Zscaler GovCloud Applicability – Access Control

AC

ZIA GOV

- Manages access by authorized users through a SaaS service.
- Controls what activities a user can perform on cloud apps via CASB.
- Leverages IDP context when building access policies.
- Encrypts all data to the Zero Trust Exchange, assuming lowest level of security.
- Monitors and controls all connections as full proxy.
- Routes all on prem and remote traffic.
- Creates deny rules based on location.
- Fully controls any outbound connections to external systems.
- Ensures controlled information does not get accessed by unauthorized users on cloud applications.

ZPA GOV

- Encrypts all data to the Zero Trust Exchange, assuming lowest level of security.
- Monitors and controls all connections as full proxy.
- Zero trust for all on prem and remote traffic.
- Allows for posture checks for remote admins prior to access.
- Limits internal user access to external systems.
- Fully controls who can access applications that contain CUI data.
- Shows application and server locations as they are requested by users.

Zscaler GovCloud Applicability – Audit & Accountability

AU

ZIA GOV

- Logs all transactional data from user to service.
- Maintains and provides access to audit logs for a year.
- Provides in depth logging and analytics for multiple security tools to one log feed and automated dashboard and report generation users on cloud applications.

ZPA GOV

- Logs all connections at a trans-actional level including user/device/app/location.
- Maintains and provides access to audit logs for a year.
- Provides in depth logging and analytics for multiple security tools to one log feed and automated dashboard and report generation.
- Shows application and server locations as they are requested by users.

Zscaler GovCloud Applicability – Configuration Management

CM

ZIA GOV

- Supports Blacklisting; Blocks application by default.
- Granular application - Whitelisting control.

ZPA GOV

- Supports Blacklisting; Blocks application by default.
- Granular application whitelisting control.
- Ensures Zero Trust Access (443) for every port opened outbound to network.
- Shows application and server locations as they are requested by users.

Zscaler GovCloud Applicability – Audit & Accountability

IA

ZIA GOV

- Limits access of identified users to specified resources stored in the cloud.
- Validates identity before granting access to the resource.
- Supports the IdP's enforcement of passwords
- Supports the enforcement of multifactor authentication capability before granting access to any user.

ZPA GOV

- Controls access by identified users to specified private applications.
- Validates identity before granting access to the resource.
- Supports the IdP's enforcement of passwords.
- Supports the enforcement of multifactor authentication capability before granting access to any user.
- Configures device posture profiles.

Zscaler GovCloud Applicability – Incident Response

IR

ZIA GOV

- Supports detection and reporting of events as part of CISCP and DIB-CS.
- Supports tracking, documenting, and reporting of incidents to designated officials.
- Supports a Security Operations Center (SOC) capability that facilitates a 24/7 response.
- Supports the use of manual and automated, real-time response to anomalous activities.

ZPA GOV

- Supports detection and reporting of events as part of CISCP and DIB-CS.
- Supports tracking, documenting, and reporting of incidents to designated officials.
- Supports a Security Operations Center (SOC) capability that facilitates a 24/7 response.
- Supports the use of manual and automated, real-time response to anomalous activities.

Zscaler GovCloud Applicability – Risk Management

RM

ZIA GOV

- Catalogs and periodically updates threat profiles and adversary Tactics, Techniques & Procedures (TTPs).
- Employs threat intelligence for the development of system architecture, selection of security solutions, monitoring, threat hunting and response and recovery activities.

ZPA GOV

- Catalogs and periodically updates threat profiles and adversary Tactics, Techniques & Procedures (TTPs).
- Employs threat intelligence for the development of system architecture, selection of security solutions, monitoring, threat hunting and response and recovery activities.

Zscaler GovCloud Applicability – System & Communications Protectione

SC

ZIA GOV

- Forwards traffic to the ZIA cloud using IPSec or TLS with FIPS validated cryptography.
- Scans for the exfiltration of sensitive traffic through DLP & CASB.
- Denies network communications traffic by default and allows network communications traffic by exception.
- Prevents unintended data exfiltration through intelligent traffic routing.
- Implements cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission.
- Terminates network connections at the end of the sessions or after a defined period of inactivity.
- Protects the authenticity of communications sessions.
- Logically isolates all network traffic.
- Completely isolates access to a CUI environment for approved SaaS's.
- Enforces port and protocol compliance.
- Fully monitors and controls the system from the internal to the external boundaries.

ZPA GOV

- Enforces port and protocol compliance.
- Fully monitors and controls the system from the internal to the external boundaries as a full security stack.
- Redefines organizational boundaries based on the users need and threat landscape with their Zero Trust Exchange approach.

Zscaler GovCloud Applicability – System & Information Integrity

SI

ZIA GOV

- Uses threat indicator information to inform intrusion detection and threat hunting as a part of CISCP and DIB-CS.
- Immediately updates malicious code protection mechanisms when new releases are available.
- Provides AV scans on every external transaction including SSL B/I encrypted traffic.
- Logs all outbound and inbound activity from ZIA assets.

ZPA GOV

- Logs all outbound and inbound activity from ZPA assets.
- Configures device posture profiles.

Zscaler GovCloud Core Services and Related CMMC Domains

AC AU SC

Advanced Firewall

Protect users connecting to the Internet with application visibility and user access-level controls for all ports and protocols.

AC AU SC

Full DNS Security (including DNSSEC and DNS tunneling)

DNS Tunneling can be used to circumvent traditional security measures and has the potential to introduce a variety of hazards into networks. To counteract this threat, Zscaler has introduced the ability to detect, control, and analyze tunneling traffic.

IR AU SC

Advanced Cloud Sandbox

Complete Behavioral Analysis (BA) engines that implement non-signature-based protection against zero-day exploits. Patient "Zero" protection with your Sandbox policy is configured to allow and scan files for the first-time action. This Zscaler service blocks users from downloading unknown files until the file is sent to the Sandbox for behavioral analysis. If a file is found to be malicious, this becomes a patient 0 event.

IR AC SC

URL Filtering

Protect your organization from harmful URLs using granular policies that specify who can access what when, where, and how.

IR SC AC AU

Cloud Application Control (CASB)

Manage access to cloud applications like webmail, streaming media, social networking, and instant messaging with granular policies that specify who can access what when, where, and how.

IA SI
AC AU

Data Loss Prevention (DLP)

Protect data across devices and networks to ensure data locality, data privacy, and regulatory requirements are met through granular controls - ensuring that data does exfiltrate the CMMC-defined boundary for the organization.

IR
AU SC

Nanolog Streaming Service (NSS)/Log Streaming Service (LSS)

Seamlessly transmit web and firewall logs from the Zscaler cloud to the enterprise security information and event management (SIEM) in real time like Sentinel, Splunk, IBM, Radar and more. Tight integration with best of breed SIEM providers with the Zscaler Splunk App which provides detailed dashboards and reporting for all Zscaler products including the ingest DLP incident information, bringing full context for DLP incidents directly into Splunk.

IR
AU SI

Private Service Edge (PSE)

Deploy to extend Zscaler's cloud architecture to the Agency premises using virtual machines (recommended only for Agencies with specific regulatory or connectivity requirements).

Conclusion

Zscaler can assist an organization in transforming their IT security environment to be highly adaptive to the new threat landscape, as well as provide a modernized approach to meet US federally-regulated accreditations, like CMMC. As the community witnesses CMMC take a more foundational approach to DOD acquisition processes relative to improving DIB security, it is increasingly plausible that other US federal agencies will follow suit and begin to put specific accreditation verbiage in their Request for Proposals (RFPs). Therefore, all companies that work with the federal government should look attentively on how the CMMC program is rolled out, how other federal agencies start following suit, and more importantly, start building their IT architecture with a Zero Trust Exchange model to account for these requirements.

About Landers and Company (L&C):

L&C is a specialized cybersecurity consultancy with a team of expert advisors providing strategic guidance and tactical implementation support for public and private sector organizations. One of our primary core competencies relates to Cloud Security compliance, specifically with the Federal Risk and Authorization Management Program (FedRAMP) and Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG), and more recently the Cybersecurity Maturity Model Certification (CMMC) as we became a Registered Provider Organization (RPO). Our experts have provided critical support to commercial entities resulting in successful authorizations to operate (ATO) at the FedRAMP Moderate and High baselines as well as the Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) Impact Levels 4 and 5. We work diligently with our clients to plan for and implement robust and comprehensive continuous monitoring programs that facilitate a dynamic and ongoing authorization process. By leveraging a flexible risk-based approach we help our clients make real progress towards efficient and integrated security programs.

Disclaimer:

L&C and Zscaler explicitly disclaim all liability concerning the use, distribution or application of the Zscaler CMMC Use Case described herein. The contents of this evaluation, the supporting CMMC controls mapping, and the application of CMMC controls to Zscaler capabilities as outlined do not guarantee CMMC certification for customers that leverage Zscaler solutions. The contents of this document are subject to change and do not represent any legal claim or guarantee of CMMC compliance. This document does not represent an attestation from an accredited CMMC Third-Party Assessor Organization (C3PAO) or an independent assessment of Zscaler solutions within a customer's CMMC boundary. L&C and Zscaler encourage all Organizations Seeking Certification (OSC) to review the contents of this document as it applies to the use of Zscaler products and engage with an RPO or C3PAO for advisory support in planning for CMMC compliance as the scope of CMMC for each organization is different and may require additional solutions to adequately protect and maintain CUI.

Appendix A: What is CMMC?

CMMC is a certification process developed by the Department of Defense to ensure that any contractors have a unified cybersecurity standard system for protection of sensitive data, including Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The intent is to incorporate CMMC into Defense Federal Acquisition Regulation Supplement (DFARS) and use it as a requirement for contract award. The CMMC Model leverages multiple sources and references of best practices from various cyber security standards, including NIST 800 Standards, Federal Regulations, Defense Federal Acquisition Regulations Supplement (DFARS), UK's Cyber Essentials and Australia Cyber Security Centre Essential Eight[1]

Unlike NIST SP 800-171, the CMMC model possesses five levels. Each level consists of practices and processes as well as those specified in lower levels. The CMMC Model v1.0 organized processes and practices into a set of domains. Process maturity, or process institutionalization characterizes the extent to which an activity is embedded or ingrained in the operations of the organization. Practices are activities performed at each level for that domain. The CMMC Model encompasses 17 Capability Domains and five levels with which to measure cybersecurity maturity.

CMMC Levels 1-3 encompass the 110 security requirements specified in NIST SP 800-171 rev1. CMMC incorporates additional practices and processes from other standards, references, and/or sources such as NIST SP 800-53, Aerospace Industries Association (AIA) National Aerospace Standard (NAS) 9933 "Critical Security Controls for Effective Capability in Cyber Defense", and Computer Emergency Response Team (CERT) Resilience Management Model (RMM) v1.2.

[1] https://www.cmmiconsultantblog.com/cmmi-faqs/what-is-cmmc-the-new-cybersecurity-maturity-model-certification-from-dod-with-latest-updates

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com