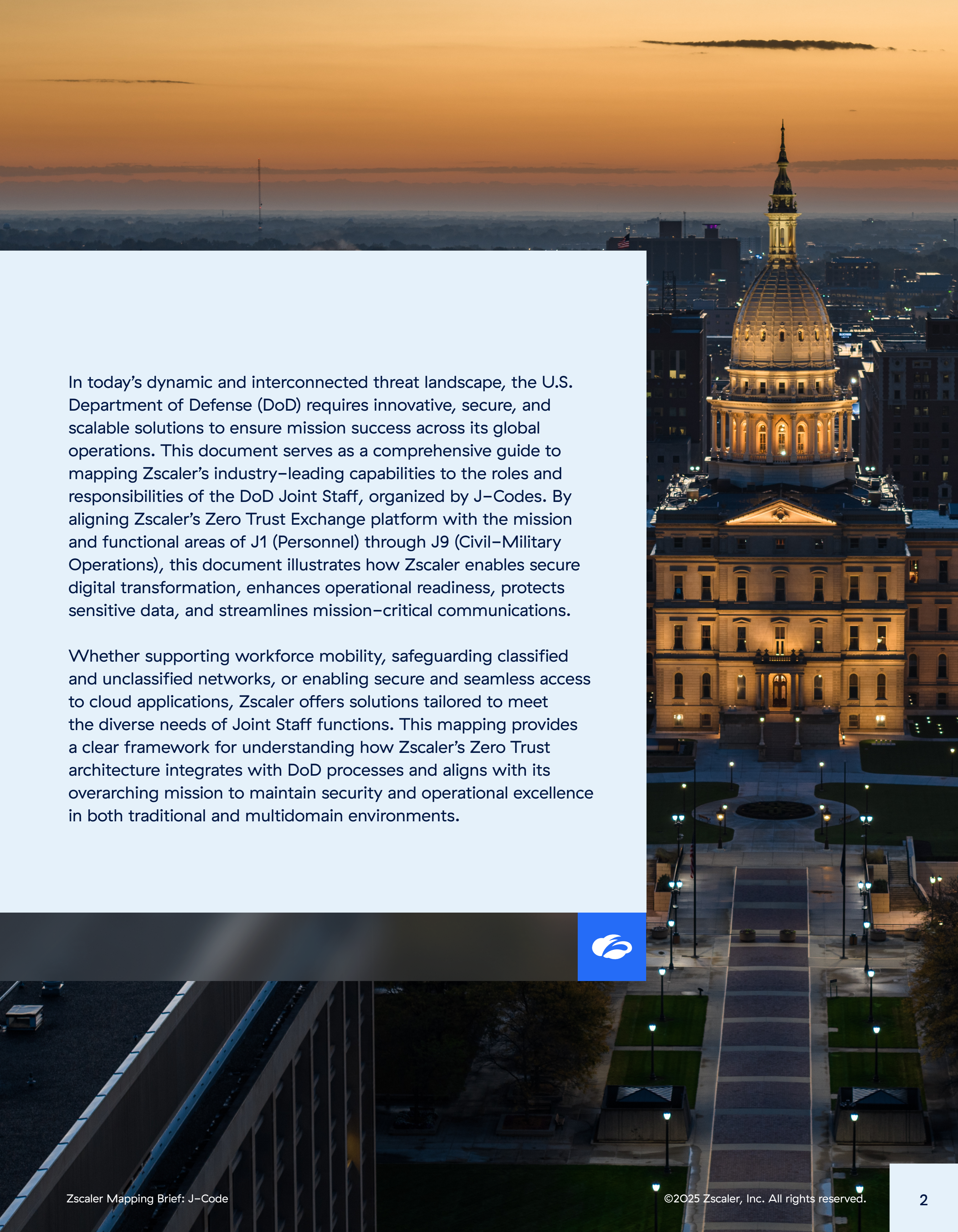# Zscaler Mapping Brief: J–Code

Mapping Zscaler Capabilities
to U.S. Department of
Defense J–Codes

In today's dynamic and interconnected threat landscape, the U.S. Department of Defense (DoD) requires innovative, secure, and scalable solutions to ensure mission success across its global operations. This document serves as a comprehensive guide to mapping Zscaler's industry–leading capabilities to the roles and responsibilities of the DoD Joint Staff, organized by J–Codes. By aligning Zscaler's Zero Trust Exchange platform with the mission and functional areas of J1 (Personnel) through J9 (Civil–Military Operations), this document illustrates how Zscaler enables secure digital transformation, enhances operational readiness, protects sensitive data, and streamlines mission–critical communications.

Whether supporting workforce mobility, safeguarding classified and unclassified networks, or enabling secure and seamless access to cloud applications, Zscaler offers solutions tailored to meet the diverse needs of Joint Staff functions. This mapping provides a clear framework for understanding how Zscaler's Zero Trust architecture integrates with DoD processes and aligns with its overarching mission to maintain security and operational excellence in both traditional and multidomain environments.

J Code Use Cases

J2 (Intelligence)

This J-Code is responsible for military intelligence, including collecting, processing, and safeguarding sensitive data to support mission-critical decision-making.

1. **Enforcing Data Loss Prevention (DLP) for Intelligence Datan**
   Zscaler ensures that intelligence analysts can access sensitive systems securely without risking the exfiltration or leak of classified data. Its DLP capabilities actively monitor and prevent unauthorized data movement.

2. **Threat Intelligence Sharing Across Agencies**
   Zscaler facilitates secure communications between intelligence organizations (e.g., NSA, DIA) and operational commands, ensuring the confidentiality of sensitive intelligence as it moves across networks.

3. **Protection Against Advanced Persistent Threats (APTs)**
   Zscaler provides Zero Trust-based protection to guard against cyberespionage by inspecting encrypted traffic and applying strict security controls, stopping adversaries from compromising intelligence systems.

J3 (Operations)

J3 oversees operational planning and mission execution, ensuring real-time coordination and situational awareness across forces.

1. **Secure Communication for Tactical Edge Operations**
   Zscaler enables secure, reliable connectivity for forces operating in austere or forward-deployed areas by leveraging Zero Trust principles, ensuring protection of mission-critical applications and networks..

2. **Enabling Coalition and Joint Operations**
   Zscaler allows real-time, secure collaboration between U.S. forces, allied nations, and other interagency stakeholders, ensuring operational decisions are made with up-to-date and accurate information.

3. **Rapid Cyber Threat Mitigation**
   Zscaler's real-time monitoring and analytics help J3 teams rapidly detect and contain cyber incidents, supporting mission continuity for time-critical operations.

J4 (Logistics)

J4 handles resources and logistics in support of military operations, ensuring supply chain effectiveness and operational readiness.

1. **Securing the DoD Supply Chain**
   Zscaler secures third-party contractor and supply chain connections to DoD networks, ensuring compliance with Cybersecurity Maturity Model Certification (CMMC) mandates and protecting sensitive logistics data.

2. **Real-Time Tracking of Logistics Systems**
   Zscaler ensures that logistics teams accessing cloud-based tracking systems (e.g., transportation or inventory management) do so securely, preventing disruptions or tampering by threat actors.

3. **Safeguarding Procurement Data**
   Zscaler protects the integrity and confidentiality of acquisition and procurement processes against cyber threats, ensuring continuity of critical logistics during mission execution.

J5 (Plans and Strategy)

J5 focuses on the development of operational plans and strategies, including policies and future readiness initiatives.

1. **Secure Collaboration on Strategic Policies and Plans**
   Zscaler enables cross–organizational and interagency collaboration on strategic planning documents, ensuring secure and reliable communication across various stakeholders.

2. **Protecting Classified and Long–Term Policy Data**
   Zscaler prevents unauthorized access and data exfiltration of long–term DoD strategic policies, leveraging Zero Trust Network Access (ZTNA) and data loss prevention capabilities.

3. **Ensuring Reliable Access for Remote Planners**
   Zscaler provides J5 teams working in distributed or remote environments with secure access to internal resources and planning tools without requiring legacy VPNs, improving both efficiency and security.

J6 (Command, Control, Communications, and Computers)

J6 manages DoD's IT infrastructure and communications systems, ensuring robust and secure digital networks.

1. **Enabling Secure Hybrid Cloud Access**
   Zscaler ensures that J6 teams can securely access mission–critical applications hosted in multi–cloud or hybrid cloud environments (e.g., AWS GovCloud, Azure Government) through granular access controls.

2. **Implementing Zero Trust Architecture (ZTA) for DoD IT Systems**
   Through continuous user verification, least–privilege access, and segmentation of resources, Zscaler supports J6 in meeting DoD Zero Trust mandates such as those outlined in Executive Order 14028.

3. **Enhancing Global Communication Resilience**
   Zscaler provides secure, high–performance global connectivity for J6–managed systems, enabling seamless communication even in bandwidth–constrained, high–latency operational environments.

J7 (Training and Education)

J7 is responsible for the training, readiness, and professional development of DoD personnel.

1. **Secure Access to Online DoD Training Platforms**
   Zscaler ensures secure connectivity for military personnel accessing cloud–based education systems, guaranteeing that their activities remain protected and private.

2. **Protecting Training Data and Records**
   Zscaler secures sensitive data such as training records, personnel evaluations, and certifications, ensuring that confidentiality and integrity requirements are met.

3. **Supporting Live Virtual Constructive (LVC) Environments**
   Zscaler enables secure real–time simulation and virtual training exercises by safeguarding communications between distributed training networks and systems.

J8 (Force Structure, Resources, and Assessment)

J8 focuses on budgeting, resource allocation, and assessment of operational needs to maintain readiness and capability.

1. **Reduction of Infrastructure Costs Through Cloud-Based Security**
   Zscaler eliminates the need for costly on-premises security appliances and reduces MPLS expenses through secure cloud-delivered services, improving the efficiency of resource allocation.

2. **Auditing Compliance with Security Standards**
   Zscaler's robust reporting and monitoring capabilities assist J8 with adhering to frameworks like DoD Risk Management Framework (RMF) and FedRAMP High, ensuring all resourcing activities comply with security mandates.

3. **Resource Planning in Classified Environments**
   Zscaler secures communications for J8 teams coordinating with contractors, allied partners, and DoD agencies on classified resource planning missions, all while supporting compliance with CMMC and other regulations.

Experience your world, secured.™