



The information provided in today's briefings is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems, or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

Cyber Security & Analytics

Zero Trust Transformation (Thunderdome)

Security Enablers

- Software Defined Enterprise
- Identity, Credential, and Access Management
- Public Key Infrastructure
- Cyber Exchange
- Cyber Training

Endpoint Security

- Endpoint Security Solution
- Comply to Connect
- Enterprise Patch Management System
- Automated Continuous Endpoint Monitoring
- Digital Policy Management System
- User Activity Monitoring
- Enterprise Mission Assurance Support Service
- Assured Compliance Assessment Solution
- Asset Inventory Management Module

JRSS

- Joint Regional Security Stacks (JRSS)
- Regional Stack Deployment and Implementation
- User Migrations
- Operational/User Training
- Cyber Operations
- Engineering, Architecture, and Integration
- Testing

Perimeter Security

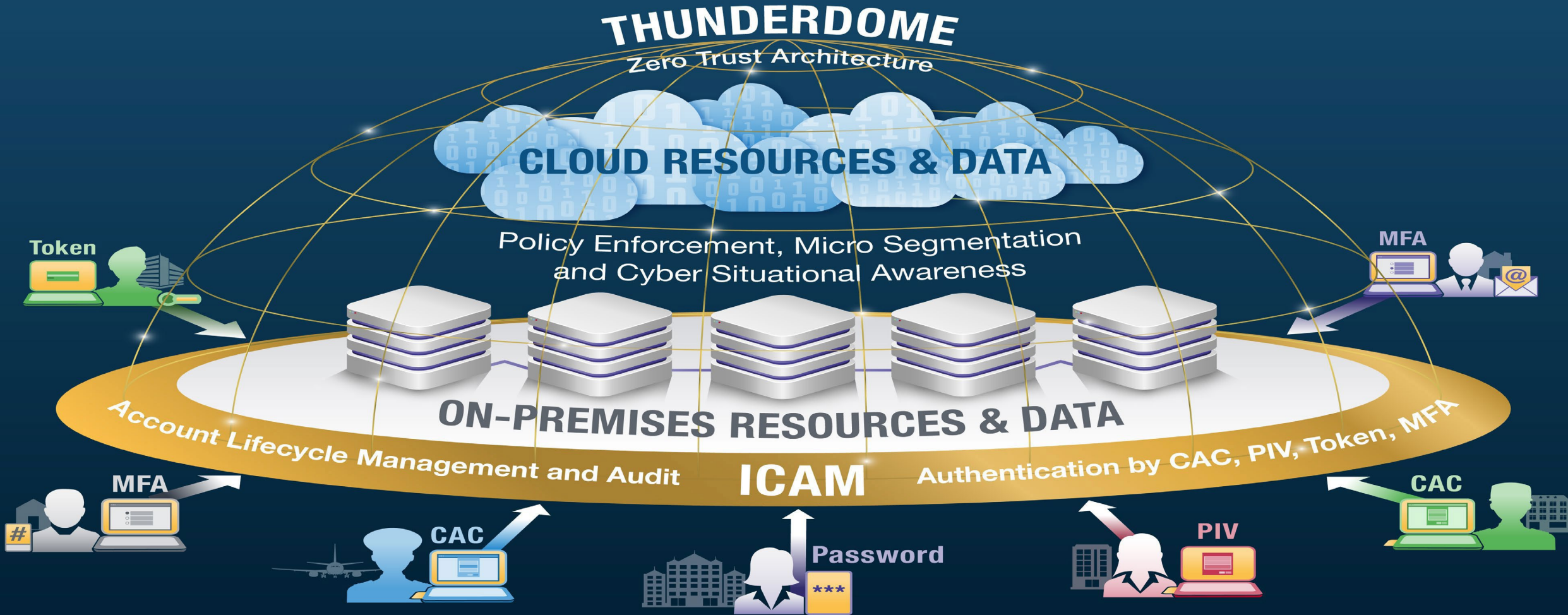
- Sharkseer
- Cross Domain Enterprise Service
- Web Content Filter
- Enterprise Break & Inspect
- Filter List Management
- Distributed Denial of Service
- Enterprise Email Security Gateway
- Zero Day Network Defense
- Domain Name System Hardening
- NIPRNet Federated Gateway
- SIPR FED/REL DMZs
- Cloud Based Internet Isolation (CBII)

Cyber Analysis and Data Sharing

- Big Data Platform
- Security Information and Event Manager
- Acropolis
- Analytics
- Continuous Monitoring and Risk Scoring
- Enterprise Sensing
- Joint Incident Management System
- Unified Cyber Situational Awareness
- DIBNet

Transform Cybersecurity Architecture to Improve Agility and Resilience with the following key principles: isolation, containment, redundancy, layers of defense, least privilege, situational awareness, and physical / logical segmentation of networks, services, and applications.

DISA Zero Trust - Enterprise ICAM & Thunderdome



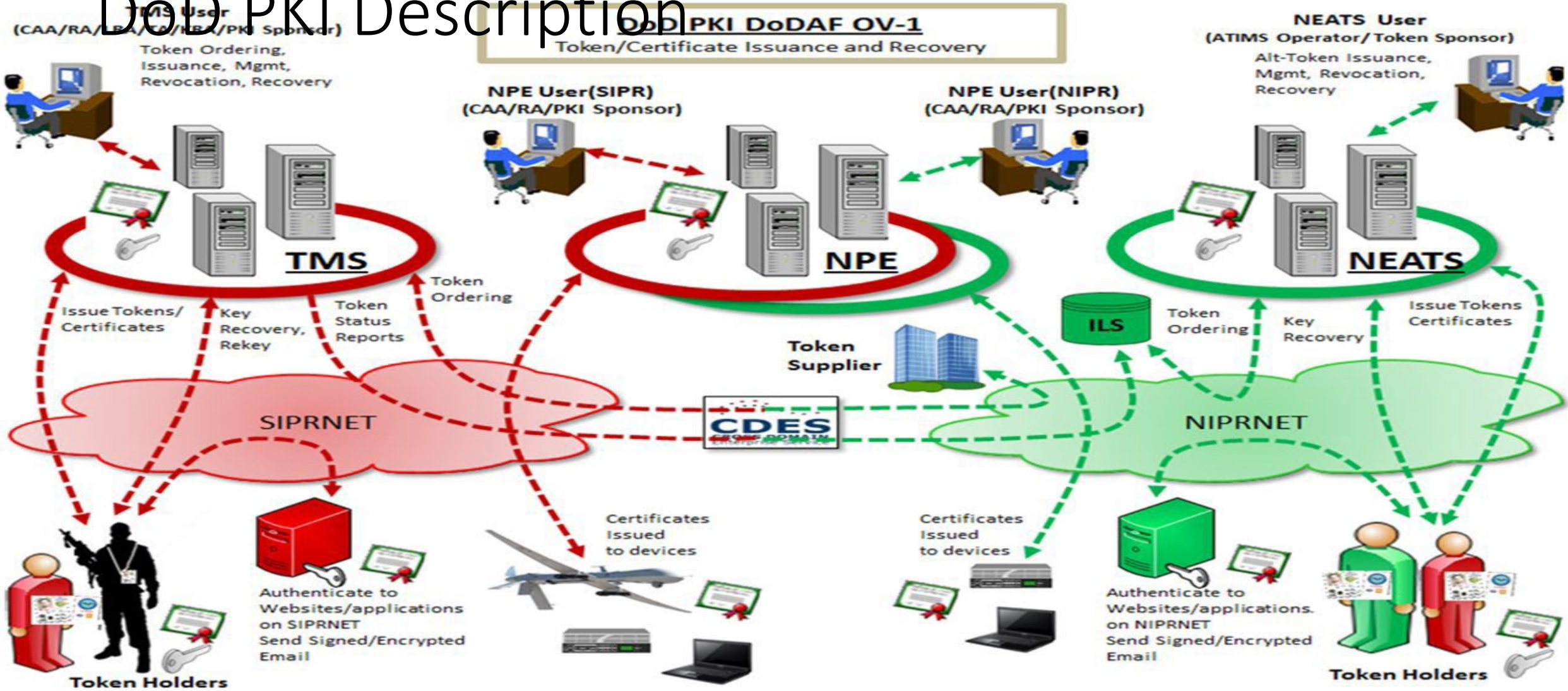
Enterprise ICAM is a foundational, enabling component of Zero Trust and DISA's Thunderdome implementation



Security Enablers Strategic Vision

- Modernize DoD PKI Systems and Applications into a Hybrid Cloud Environment
- Optimize the DoD PKI Program for Efficiencies and Improved Capabilities.
- Deploy Insider Threat Detection Capabilities
- Implement Automated Patch Management
- Enhance Cybersecurity Situational Awareness through Big Data Analytics
- Expand the use of Derived Credentials
- Cryptographic Modernization

DoD PKI Description



Endpoint Strategic Vision

- Improve Endpoint Security and Continuous Monitoring
- Establish Enterprise Comply-to-Connect Capability
- Deploy Insider Threat Detection Capabilities
- Implement Automated Patch Management



Perimeter Security Strategic Vision

- Implement Zero Trust capabilities that align with the DoD Zero Trust Reference Architecture
- Protect the DoD Information Network from Web and Email threats
- Field life cycle support for cross domain solution technologies that provide secure interoperable capabilities throughout the Department of Defense (DoD)



Acquisition Opportunities FY23 & Beyond



Project Title & Description	Program Office	RFP / Projected Award
Demilitarized Zone (DMZ) -Engineering & Program Management Support Provide program management, engineering and Tier III support for the DMZ portfolio.	DISA DCSC ID5	Single Award Full and Open RFP 4Q FY23 Award 1Q FY24
Domain Name Service (DNS) Hardening Engineering Support Provides engineering support services for the DNS.	DISA DCSC ID5	Single Award TBD RFP 4Q FY23 Award 1Q FY24
Cross Domain Enterprise Services (CDES) Program Management and Engineering Support Provide Department of Defense (DoD) consolidated enterprise-wide cross domain solution. CDES provides hardware, software, and related support for the transfer of information between DoD classified and unclassified networks with high assurance, speed, and integrity.	DISA DCSC ID5	Single Award Small Business Set- Aside RFP 2Q FY24 Award 4Q FY24



Project Title & Description	Program Office	RFP / Projected Award
<p>Cyber Development Directorate Professional Services Portfolio Support Expertise and comprehensive acquisition, portfolio management, and business office support to the DISA ID Offices and supported portfolios.</p>	DISA DCSC ID1	Single Award TBD RFP 2Q FY23 Award 3Q FY23
<p>Assured Compliance Assessment Solution (ACAS) Support Operate and sustain the current ACAS enterprise solution. Support integration with evolving DoD requirements.</p>	DISA DCSC ID3	Single Award TBD RFP 1Q FY24 Award 3Q FY24



Project Title & Description	Program Office	RFP / Projected Award
Domain Name Service (DNS) Hardening Engineering Support Provides engineering support services for the DNS.	DISA DCSC ID5	Single Award TBD RFP 4Q FY23 Award 1Q FY24
Gateway Security Engineering Support Provides gateway computer network defense systems for internet to NIPRNET gateway protection, detection, and response.	DISA DCSC ID5	Single Award Full and Open RFP 3Q FY24 Award 1Q FY25
Cloud Based Internet Isolation Mitigate the DoD Information Network (DoDIN) threats and free up bandwidth capacity, by redirecting Internet browsing from the end user's desktop into a remote cloud-based server.	DISA DCSC ID5	Single Award OTA RFP 4Q FY24 Award 2Q FY25



Project Title & Description	Program Office	RFP / Projected Award
<p>SharkSeer Cybersecurity Engineering and Sustainment Provides migration, integration, testing, O&M, improvement, streamlining, optimization, enhancement, and simplification of all SharkSeer functionalities across seven operational boundaries, together which identify and mitigate zero-day attacks and advanced persistent threats to protect the DoD.</p>	DISA DCSC ID5	Single Award Full and Open RFP 2Q FY25 Award 4Q FY25
<p>Web Content Filtering Engineering and Sustainment Support To scan and block malicious inbound and outbound traffic at the Non-Secure Internet Protocol Router Network (NIPRNet)/Internet Gateways.</p>	DISA DCSC ID5	Single Award Full and Open RFP 2Q FY25 Award 4Q FY25



Project Title & Description	Program Office	RFP / Projected Award
<p>Defense Industrial Base Network Developing, sustaining and maintaining the current operational capabilities of the DIBNet-U, DIBNet-S, and Incident Collection Form (ICF).</p>	<p>DISA DCSC ID6</p>	<p>Single Award Encore III RFP 1Q FY25 Award 3Q FY25</p>



Information

www.disa.mil

Contracting Opportunities

www.sam.gov