








Services	Current State	FY 23			FY 24				FY 25 +	Future State
		Q2	Q3	Q4	Q1	Q2	Q3	Q4		
<b>Application</b>  <p>Application protections are inconsistently applied across the enterprise</p>	<p><b>API</b></p> <p>Exemplar API use cases identified</p> <p>Risk Management Strategy</p> <p>Current state Application ecosystem inventoried</p> <p>Monitor Mode Data Flow Mapping initiated</p> <p>Macro Segmentation</p>	<p>API strategy published and 'shared service product' defined</p> <p>Enterprise SBOM Strategy published</p> <p>Enterprise SBOM</p> <p>PACAF SDP Pilots deployed</p>	<p>Common SBOM repository completed, and viable assessment tools identified</p> <p>Data Flow Mapping initiated for Enforcement Mode</p> <p>BIM SDP phased rollouts initiated</p>	<p>80% of Enterprise Application Inventory published</p> <p>SASE Solution services IOC deployed</p> <p>SDP for VPN replacement viable for user subgroup</p>	<p>DevSecOps API services IOC deployed</p> <p>Micro operationalized</p> <p>Ongoing application configuration</p> <p>JRSS sunset completed</p>	<p>Standardized security control measures across enterprise applications</p>				
<b>Network</b>  <p>VPN as the primary tool to secure remote access, combined with legacy network practices</p>	<p>Micro Segmentation</p> <p>SDP</p>	<p>Enterprise SBOM Strategy published</p> <p>PACAF SDP Pilots deployed</p>	<p>Common SBOM repository completed, and viable assessment tools identified</p> <p>Data Flow Mapping initiated for Enforcement Mode</p> <p>BIM SDP phased rollouts initiated</p>	<p>SASE Solution services IOC deployed</p> <p>SDP for VPN replacement viable for user subgroup</p>	<p>80% of Enterprise Application Inventory published</p> <p>SDP for VPN replacement viable for user subgroup</p> <p>Micro operationalized</p> <p>Ongoing application configuration</p>	<p>Fully enforced micro segmentation with generally available SASE solution with SDP solution deployed at base level and tailored to application level</p>				
<b>Devices</b>  <p>Devices are managed locally and device health systems are disconnected from authorization decisions</p>	<p>C2C</p> <p>Device Inventory</p> <p>Device Health</p>	<p>Existing C2C solutions inventoried and mapped to DoD mandate</p> <p>Device 4 Life Strategy published</p>	<p>C2C Strategy and reference architecture published</p> <p>EITaaS Wave 1 Help Desk and ITSM deployed</p> <p>Cloud-based XDR Platform deployed on NIPR for traditional and EITaaS devices</p>	<p>C2C implementation plan approved</p> <p>SDP and SASE continuous authentication best practices published</p>	<p>Cloud-based XDR Platform deployed on NIPR for traditional and EITaaS devices</p> <p>Cloud-based XDR integrated with SDP</p> <p>Cloud-based XDR deployed for all environments</p>	<p>Automated and cloud-based tools that manage device health and feed access decisions with Device 4 Life rolled out</p>				
<b>Continuous Monitoring</b>  <p>Current generation Defense Cyber Operations (DCO) focuses on network-centric monitoring</p>	<p>SIEM/SOAR</p>	<p>Application events and SIEM/SOAR integration initiated for FIAR audit remediation</p>	<p>Logs and data necessary for continuous monitoring identified</p>	<p>Shared responsibility model for application events with CSSPs published</p>	<p>Logs, processes, and data available for CSSPs and SOCs formally established</p>	<p>Continuous Monitoring for applications fully scaled and integrated into operations</p>				
<b>Policy</b>  <p>Ongoing discovery and development of best practices across application and data security ecosystem</p>	<p>PDP/PEP and all policy related tasks</p>	<p>Risk acceptance policy for Managed vs. Unmanaged Devices published</p>	<p>Reference architecture for various PDP/PEP ecosystems published</p>	<p>Policy for leveraging major vendors for behavioral analytics published</p>	<p>Joint User Device Health Strategy published</p>	<p>Policies developed, implemented, and enforced supporting industry and DoD best practices</p>				
<b>User</b>  <p>Inconsistent &amp; inadequate authentication and access management by each financial and financial feeder system</p>	<p>Reference ICAM Roadmap</p>	<p>FIAR ICAM activities initiated</p>	<p>Enterprise ICAM IOC deployed</p>	<p>Enterprise ICAM FOC deployed</p>	<p>Ongoing transition to attribute-based identity and continuing application integrations</p>	<p>Deployed single enterprise ICAM solution serving all communities and environments with enhanced authentication and controls</p>				
<b>Data</b>  <p>Leveraging Big 6 data platform for operational outcomes and continuously maturing</p>	<p>Data</p>	<p>Data Fabric Roadmap published</p>	<p>Lessons learned from NC3 assessed</p>	<p>Core tagging and labeling tools baselined</p> <p>NPE and data platform integration initiated</p>	<p>Access attributes for data baselined</p> <p>Ongoing data integrations with major data platforms</p>	<p>Data and API services fully integrated and supported by Enterprise ZT services (e.g., NPEs)</p>				