Zero Trust Driving the Upgrade of BUMED's Identity, Credential, and Access Management Strategy

by Greg Rosoff and Nirali Chawla

As federal agencies continue to build out zero trust architecture (ZTA), they have been focusing in on a critical component to any zero-trust strategy: identity, credential, and access management (ICAM) solutions. ICAM will help to resolve identity and access management deficiencies and move the Department of Defense (DoD), including the Navy Bureau of Medicine and Surgery (BUMED), toward a modern and resilient cybersecurity approach focused on networks, users, devices, and data.

While BUMED recognizes the importance of and awaits an enterprise-wide ICAM solution/capability, we similarly recognized the need o develop and implement an interim BUMED ICAM strategy focused on upgrading its current identity and access management business processes. As part of the ICAM strategy, BUMED developed and adopted its own cutting-edge identity and access management tool (Terminations, Information Awareness Training, Clearance, and Recertification and Segregation of Duties (TICRS)), to provide robust security without compromising the user experience.

The TICRS tool currently captures over 150 million data points related to over a million BUMED and Defense Health Agency system user-name/role combinations including their organization, system, email, supervisor information, clearance status, and training compliance. The TICRS tool's user-friendly front-end interface, presents information in a clear and accessible format, simplifying the entire BUMED user management (UM) process and enabling streamlined access management. This UM process includes onboarding new BUMED employees, privileges they receive, how these privileges evolve over time, and offboarding separated/terminated BUMED employees. The TICRS tool modernizes BUMED's identity management processes. It achieves this by actively managing user access permissions, requires regular supervisory verification for system access, tracks clearance eligibility and Information/Cyber Awareness training status. It also highlights non-compliant user system roles (e.g., access privileges granted are not appropriate to role and/or access is granted to terminated BUMED employee).

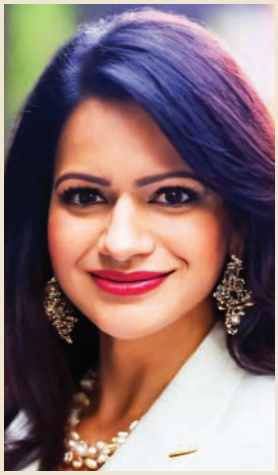
"The TICRS tool allows BUMED to improve its cybersecurity posture and address these critical deficiencies by permitting supervisors to continuously review and monitor user access privileges with built-in auditing to ease compliance processes."

Access controls and segregation of duties are critical areas the independent auditors review every year. The ability to restrict logical access to active individuals, review user/privileged user system access, identify incompatible duties, continuously identify least privilege access, and deploy risk mitigation all continue to be critical DoD deficiencies reported by independent auditors. The TICRS tool allows BUMED to improve its cybersecurity posture and address these critical deficiencies by permitting supervisors to

continuously review and monitor user access privileges with built-in auditing to ease compliance processes. Future TICRS tool enhancements include an interface with business intelligence tools to provide additional analysis and insights to stakeholders and leadership for executive decision-making.

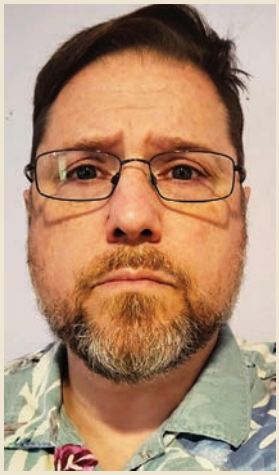
If your federal agency is looking to upgrade its identity and access management strategy, solutions, and practices, contact Mr. Rosoff or Mrs. Chawla points of contact to learn more about the TICRS tool development, implementation, and how it might be suitable for your organization. By taking the necessary steps to properly integrate the TICRS tool into your ZTA, it will improve your UM process, security, user experience, controls, and reduce risks and compliance costs. The TICRS tool could be just the solution needed to take your federal agency's identity and access management to the next level!

The views expressed in this journal article are those of the authors, Greg Rosoff (BUMED N81-gregor.a.rosoff.civ@health.mil) and Nirali Chawla (KPMG, niralichawla@kpmg.com), and do not necessarily reflect the official policy or position of the Department of the Navy, Department of Defense, the U.S. government, nor KPMG.



Nirali Chawla

Nirali Chawla is a Managing Director within KPMG'S Federal Practice. She is the leader of the Tech Risk Management service network and has over 20 years' experience supporting organizations with IT audit, IT audit readiness, and IT modernization efforts. Nirali is a certified CISA, CRISC, CISSP and CAP professional.



Greg Rosoff

Greg Rosoff has experience in the commercial sector, Department of Defense, and as a federal civilian in a variety of financial and IT roles. He currently leads the Navy Bureau of Medicine and Surgery's FISCAM-compliance efforts.