maximus

Bridging the Cyber Skills Gap: A Workforce Development Imperative

Building a Resilient Cybersecurity Workforce for Federal Government

Developing a robust federal cybersecurity workforce is crucial to protecting government systems, data, and services that support critical public programs. A well-trained cybersecurity workforce can defend against increasingly sophisticated cyber threats, safeguard critical infrastructure, and maintain public trust in government services. Maintaining a strong federal cybersecurity workforce also plays a vital role in supporting the nation's economic strength and global position.

Maximus is collaborating with federal agency partners to develop cybersecurity talent pipelines aligned with national workforce priorities. Through internal talent development, government upskilling, public-private partnerships, academic pathways, Maximus is helping prepare robust, adaptable, and skilled cybersecurity professionals who can meet the complex and dynamic needs of federal agencies.

A robust approach to advancing the federal cybersecurity talent base

The federal cybersecurity talent pool includes current professionals in government and contracting roles, as well as emerging talent from industry, the military, Veterans, and students. Maximus considers each of these areas to support the development of federal cyber talent by:

- Helping our federal government partners ensure their cyber teams have the training and skills necessary to address today's cybersecurity landscape, and its future evolution
- Engaging in partnerships with academia, industry, and Veteran communities to advance new cybersecurity talent
- Strengthening our own talent acquisition and retention strategies to ensure our staffing for security operations centers (SOCs) meets the skills requirements of the federal government

... requires technological adaptation to mitigate risk and improve our nation's competitiveness and innovation.

Training and Upskilling Pipelines

Addressing the cybersecurity workforce shortfall also requires technological adaptation to mitigate risk and improve our nation's competitiveness and innovation. Maximus is addressing this with training and upskilling pipelines, including:

- Cybersecurity best practices for a workforce capable of effectively preventing, detecting, and mitigating cybersecurity risks
- Cybersecurity compliance training, providing skills and tools to meet and document requirements under the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), Federal Information Security Management Act (FISMA), and other federal mandates
- SOC roles and responsibilities to promote a coordinated, knowledgeable team that can efficiently and effectively respond to and mitigate cyber threats
- SOC analysts operations training, including incident handling and vulnerability management, to help ensure rapid threat remediation and enable rapid asset recovery for mission continuity
- Defining skills and certifications for analysts in collaboration with federal customers to ensure standard qualifications and benchmarks for those who work to secure government systems
- Identifying current and emerging threats and technologies, ensuring the cyber workforce can anticipate risks, adapt security practices, and understand how new tools may both mitigate and introduce vulnerabilities

Public-Private Partnerships

Maximus is actively engaging in public-private partnerships to help build talent pipelines and strengthen cybersecurity workforce development with both industry and academia.

Academic Initiatives

Academic development programs help train and inspire the next generation to enter the cyber workforce. Through initiatives with institutions including George Mason University, West Virginia University, and Marshall University, Maximus is:

Maximus leverages several programs to retain talent as they transition between contractual work...

- Providing students with learn-by-doing opportunities with projects such as cryptography, securing healthcare IT systems, internet of things (IoT) devices, and other projects with relevance to federal organizations
- Aligning student learning objectives and cybersecurity curricula with federal cyber needs and priorities
- Providing students with access to cybersecurity career mentorships for professional development
- Ensuring students learn the importance of federal cybersecurity compliance, certifications, and accreditations
- Increasing student competitiveness in the employment market
- Establishing hiring pipelines of students with modern and relevant skillsets for both federal agencies and contractors supplying cybersecurity services

Industry Partnerships and Collaboration

By working closely with strategic technology partners and industry, Maximus is building relationships aimed at advancing federal cyber capabilities, developing talent, and addressing workforce challenges. These initiatives include:

- Partnerships with leading cloud service providers, offering workforce opportunities for training and certification in FedRAMP-authorized solutions and encouraging experimentation with AI/ML and other emerging technologies to stay ahead of the curve
- Engagement with technology vendors and industry working groups to help shape cybersecurity research, provide input on needed cyber skills and technologies, and create pathways for talent development
- Participation in advisory groups including the American Council for Technology – Industry Advisory Council (ACT-IAC), collaborating alongside experts from government, industry, and academia to help shape cybersecurity best practices

Talent Identification and Retention Strategies

Maximus leverages several programs to retain talent as they transition between contractual work, including the Resource Management Board (RMB) and Project Mobility Board (PMB), to ensure that existing contracts have sufficient backfill of qualified candidates.

Team Maximus (TMAX) Depth Chart and Cross-Trained Staff

This initiative helps ensure personnel have sufficient cross-training across the team. Our depth chart covers each role and identifies the primary role, operational back-up, and additional qualified staff across who could fill the role if needed (including potential contingent hires).

Technical Focus Competencies (TFC)

This dedicated division of cyber experts at Maximus demonstrates significant technical leadership alongside other TFCs, including Software and Infrastructure, Digital, and Data Management. Each TFC comprises specialized experts within their focus area, and the TFCs are aligned under a single leader to ensure necessary integration. These experts serve as trusted advisors and proactive partners, deeply engaged in our clients' modernization journeys, ensuring responsive and forward-thinking solutions.

Project Mobility Board (PMB)

The PMB is an initiative implemented to augment the standard hiring process to match project needs to personnel available within the company. It provides a centralized way to highlight all staff openings across all projects. Recruiting starts within our internal resource pool of candidates who have already proven their capabilities and work ethic. By hiring from within, we incentivize our workforce with opportunities for career growth within Maximus.

Demonstrated Impact

As a trusted partner to federal agencies, Maximus has provided cybersecurity training and development to security teams across defense and civilian organizations. Our holistic approach to staffing and retention for the workforce supporting federal cybersecurity programs resulted in:

- 95% retention rate for Transportation Security Administration's (TSA) Computer Network Defense (CND)
- 85% retention rate for Department of Defense's highly classified Special Access Programs (SAP) within the Chief Information Officer (CIO) organization
- 94% retention rate for cybersecurity related programs at the Department of Energy's (DOE) National Energy Technology Laboratory (NETL)

From cybersecurity best practices to in-depth SOC topics, Maximus supports our federal partners in proactively navigating emerging cyber threats, adopting cutting-edge technologies, and cultivating the critical skills required to secure and sustain the federal enterprise.

Why Maximus

Operational Expertise

We leverage deep experience managing large-scale operations and data architectures to identify new vulnerabilities, secure against known threats, and ensure government mission success and compliance with current requirements.

Agillity & Innovation

Appraised at CMMI Level 5 – the highest level – for both services and development, we quickly adapt to changing requirements for continuous agility and innovation.

Secure Infrastructures

With FedRAMP Moderate Authorization for cloud environments, we provide a portfolio of managed services including infrastructure (IaaS), platform (PaaS), and software (SaaS) to meet unique government compliance and security requirements.

Technical Expertise

With our incubator environment we foster a culture of continuous learning and growth, led by a team of cybersecurity experts boasting 100+ advanced certifications.

Maximus Cybersecurity Experts

Kynan Carver
Managing Director,
Cybersecurity Technology Services

Michael Sieber
Senior Director,
Cybersecurity Technology Services

Michael Geronimo
Director,
Cybersecurity Technology Services

Certifications and Authorizations

FR FedRAMP

CMMIDEV/5℠
CMMI®V2.0 / Exp. 2022-11-29 / Appraisal #50104

CMMISVC/5℠
Exp. 2021-06-13 / Appraisal #32371

International Organization for Standardization ISO 20000

International Organization for Standardization ISO 9001

Information Security Management ISO 27001 Certified

ITIL®

PMI PMBOK

in maximus 𝕏 @maximus_news

maximus.com/technology-services/cybersecurity