**Testimony of David Powner**
**Before the Subcommittee on Technology Modernization**
**of the**
**House Veterans' Affairs Committee**
**November 20, 2024**

Chairman Rosendale, Ranking Member Cherfilus-McCormick, and distinguished Members of the Subcommittee on Technology Modernization, thank you for the opportunity to testify before you today on the Department of Veterans Affairs cybersecurity posture. MITRE is a non-profit, nonpartisan research institution that operates Federally Funded Research and Development Centers (FFRDCs) on behalf of the U.S. Government. Among other technical disciplines, our team of over 1,500 cybersecurity professionals provide deep expertise across the executive branch, including in support of organizations like the Department of Veterans Affairs, Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and U.S. Cyber Command. MITRE's ATT&CK™ framework has become the de facto language between government and industry for describing and combatting cyber threats.

Currently, I lead MITRE's Center for Data-Driven Policy. We draw upon our deep expertise on topics like engineering, acquisition, and cybersecurity to bring non-partisan, evidence-based insights to policymakers in both the legislative and executive branches. My statement today will summarize MITRE's independent cybersecurity assessment directed in the Strengthening VA Cybersecurity Act of 2022, which included a comprehensive review of five high-impact systems and an overall evaluation of the VA's Information Security Program. We delivered our report to VA on April 30, 2024. I will summarize our assessment methodology, findings, recommendations for improvements, and VA's remediation progress.

## Assessment Methodology

For the assessment, we selected 5 high-impact systems from VA's list of Bedrock and Critical Systems list based on the prescribed selection criteria, and briefed Committee staff on our selected systems to ensure that we were meeting the intent of the Act. The selected systems

were the Integrated Financial and Acquisition Management System (iFAMS), Loan Guaranty (LGY), Health Care Claims Processing System (HCPS), MyHealtheVet (MHV), and VA Enterprise Cloud – Mobile Applications Platform (VAEC-MAP). Our system assessments included vulnerability scans, configuration reviews, and software evaluations for malicious techniques, tactics, and procedures. Throughout the assessment, we immediately reported significant findings to VA for action.

For the overall evaluation of VA's Information Security Program, we leveraged NIST's Cybersecurity Framework 2.0 to ensure broad coverage across key cybersecurity capabilities. We evaluated governance, asset management, vulnerability management, configuration management, identity credential and access management, and cloud security. This included leveraging our ATT&CK™ Framework to perform threat-informed testing on operational networks, evaluating tools and configuration settings at VA's Cybersecurity Operations Center, conducting tabletop exercises on response and recovery capabilities, and evaluating shadow IT for cybersecurity risks.

**Key Findings**

Our independent assessment found that VA implemented many standard cybersecurity measures and provided fundamental levels of cybersecurity protection. Although the five systems we assessed exhibited many of the information security protection mechanisms and controls outlined in VA policy and NIST guidance, we identified findings within each system that we categorized as high, moderate, or low risk. MITRE has performed several hundred of these systems cyber assessments across various government agencies and the total number of findings was relatively consistent with other similarly-sized systems while the number of high risk findings assessed was lower than what we typically observed. It is important to note that VA remediated almost 30 percent of these systems' findings, and nearly 50 percent of the high-risk findings, by the time we submitted our final report in April. Thematic findings from these system assessments called for improvements in applying software patches; configuring

operating systems, databases, and cloud services; access controls; secure software development practices; and logging events to detect ongoing attacks.

Regarding our assessment of VA's overall Information Security Program, we found a number of systemic operational and management issues that were corroborated with past IG reports. These findings were grouped into 11 areas:

- OIS Customer Service to Systems Teams – OIS teams that provide security services to system-level teams do not effectively communicate and coordinate together, hindering effective cybersecurity implementation.
- Cybersecurity Governance – Siloed operations and outdated policies affect overall cybersecurity effectiveness.
- Cybersecurity Risk Management – Improvements are needed to mature beyond compliance activities.
- Information System Security Officer (ISSO) and System Steward Roles – ISSO roles need to be aligned with specific systems (e.g., infrastructure, medical devices).
- Continuous Monitoring – Improvements are needed in control assessments, vulnerability scanning, configuration compliance, and software management.
- Medical devices – Quickly addressing vulnerable medical devices and maintaining security over the life of these devices is a constant challenge.
- Cloud security – Cloud configurations need to be consistently applied.
- Shadow IT – Shadow IT introduces unaccounted-for risk.
- Cyber Protection – Implementing Zero Trust will further enhance protection.
- Cyber Detection – There are opportunities to optimize tools, alert triggers, and integration capabilities.
- Response and recovery – Siloed organizations and manual operations hinder VA's ability to maintain mission continuity.

**Recommendations**

We made 11 overall recommendations for the five systems we assessed, including prioritizing the remediation of the high and moderate risk systems findings. We also recommended that VA close the low-risk findings to the greatest extent possible given that the threat landscape is constantly changing, and these may evolve to higher-risk vulnerabilities over time. Other recommendations focused on applying patches, improving vulnerability scanning capabilities, and configuring systems and cloud offerings appropriately.

We made 35 recommendations to improve VA's overall cybersecurity program. Priority recommendations included:

- Enhancements to VA's risk management framework
- Developing baseline configurations and enterprise secure baseline checklists for cloud environments
- Reducing shadow IT to mitigate cybersecurity risk
- Configuring endpoint detection and response solutions to block and prevent known malicious software
- Creating alerts based on audit log events to improve visibility of high-impact events.

**Remediation Activities**

VA reports that it has closed 70 percent of our 5 systems findings and 93 percent of the high-risk findings and continues to address the 11 system and 35 overall recommendations.

In summary, I would like to commend the Committee for calling for such a comprehensive, independent review and VA's management team's commitment to constantly improving its security posture. We believe the combination of our recommendations and the ongoing improvements will significantly enhance VA's cybersecurity effectiveness, thereby strengthening the Department's ability to serve and protect America's Veterans.

On behalf of the entire MITRE team, we look forward to continuing to help VA secure and modernize their critical operations. I greatly appreciate the opportunity to come before you again today and I look forward to your questions.