

**STATEMENT OF
MR. EDDIE POOL
PERFORMING THE DELEGABLE DUTIES OF THE ASSISTANT SECRETARY FOR
INFORMATION AND TECHNOLOGY AND CHIEF INFORMATION OFFICER
OFFICE OF INFORMATION AND TECHNOLOGY
DEPARTMENT OF VETERANS AFFAIRS (VA)
BEFORE THE
COMMITTEE ON VETERANS' AFFAIRS
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION
U.S. HOUSE OF REPRESENTATIVES
ON
VA OFFICE OF INFORMATION AND TECHNOLOGY ORGANIZATIONAL
STRUCTURE AND PRIORITIES**

July 14, 2025

Introduction

Chairman Barrett, Ranking Member Budzinski, and distinguished Members of the Subcommittee, thank you for the opportunity to testify on behalf of the Department of Veterans Affairs (VA) Office of Information and Technology (OIT). I am Eddie Pool, performing the delegable duties of the Assistant Secretary for Information and Technology and Chief Information Officer (CIO). I am honored to appear before you today to provide an update on the status of OIT and the critical work we are doing to deliver secure, modern, and Veteran-centered information technology (IT) solutions. I am accompanied by my OIT colleagues, Dr. Timothy Puetz, Chief Financial Officer and Deputy CIO for IT Budget and Finance; Mr. Jack Galvin, Deputy CIO for End User Services; and Ms. Devon Beard, Acting Deputy CIO and Chief People Officer for the Office of People Science.

Let me center my remarks on three core priorities: budget modernization, workforce reshaping, and cybersecurity posture.

Budget

We are driving a bold and forward-thinking approach to budget modernization, one that matches the pace of today's technological landscape. Over the past few months, OIT has undertaken a comprehensive and rigorous review of our contracts and budget to ensure that every dollar spent delivers real value to Veterans and their families. During this process, we were able to reinvest \$89 million into the infrastructure readiness program. Furthermore, we are positioned to reinvest an additional \$100 million. The Improvement and Remediation Program (IRP) serves as the investment fund dedicated to ensuring all IT infrastructure such as endpoints, network, and datacenters is both "Fit for Purpose" through modernization efforts, and "Fit for Use" via technology refresh initiatives. In recent years, the Office of Information and Technology (OIT) has effectively leveraged the IRP to address technical debt stemming from aging systems or solutions that no longer meet current requirements.

Any contract terminations or modifications occurred after OIT assessed internal capabilities and confirmed that critical work could continue without disruption. This intentional, mission-first strategy has strengthened continuity, reduced complexity, and delivered smarter, more reliable IT capabilities. By intensifying our contract oversight and forging stronger coordination with our acquisition partners, we are decisively managing contract changes without compromising service delivery. This proactive approach not only boosts efficiency but also enables us to strategically redirect resources to mission-critical areas and emerging priorities, ensuring we remain agile and focused on delivering positive outcomes for Veterans.

OIT is vigorously working to eliminate unnecessary expenses while maintaining operational readiness. These initiatives underscore our dedication to being responsible stewards of taxpayer dollars while effectively fulfilling our mission. Where necessary, we actively reassess the use of Government-furnished equipment, cut down on unused cellular lines, and enforce stricter eligibility criteria to guarantee that resources are allocated solely to essential personnel.

We are also requesting changes to the appropriations language to allow VA to eliminate rigid statutory subaccounts and authorize a 3-year period of availability for IT funds. Granting a 3-year funding cycle will allow us to plan and execute across longer horizons, respond more effectively to real-time needs, and align investments with outcomes. These adjustments promote disciplined, results-driven investment while minimizing procurement risk and operational delays. Furthermore, we have implemented rigorous internal controls including quarterly reporting and CIO risk ratings to ensure accountability remains central.

Workforce

OIT is committed to deploying staff resources in the most effective and efficient way to better serve our Veteran community. OIT is actively engaged in workforce reshaping to ensure we assign resources to critical positions to meet the Department's mission.

We are decisively aligning every staff resource to achieve Veteran-facing outcomes. Recently, we participated in the Office of Personnel Management and VA Deferred Resignation Program/Voluntary Early Retirement Authority. Among those who voluntarily participated, 78% opted for retirement, with over 53% being Veterans who entered early retirement. This grants a unique ability to reallocate human capital to meet emerging mission needs, particularly in areas like cybersecurity and AI, thereby delivering better outcomes for Veterans. We are taking bold steps to reshape our workforce structure from nine service lines to three: Technical Operations, Product Delivery, and the Office of the Chief of Staff. This strategic realignment is designed to eliminate unnecessary bureaucracy, accelerate decision-making, and sharpen our focus on delivering innovative, impactful IT services that directly support Veterans.

To build a robust workforce, OIT is prioritizing and reallocating staff to bolster essential functions. We are aligning our onboarding efforts with mission delivery to ensure we possess the technical capacity required to meet the Department's future

needs. Our approach effectively balances immediate operational demands with long-term workforce planning, ensuring both continuity and readiness in all our endeavors.

Cybersecurity

Cybersecurity is a complex and constantly evolving threat. We are shifting our strategy toward dynamic, threat-informed defenses prioritizing proactive risk mitigation over reactive compliance. This is not just about meeting checkboxes anymore; it is about anticipating threats and acting before they happen. Federal Information Security Management Act/Federal Information System Controls Audit Manual audits must reflect the complexity of VA's digital infrastructure and the sophistication of adversaries we face. Our shift embraces dynamic, threat-informed defenses and promotes proactive mitigation over retrospective correction.

OIT is promoting Zero Trust by fostering a security-first mindset across the Department and by prioritizing the protection of critical information and resources. Zero Trust is a security model and framework that operates on the principle that no user, device, or application should be trusted by default, regardless of whether they are inside or outside an organization's network. Instead, every access request must be continuously authenticated, authorized, and validated before granting access to resources.

This approach involves rigorous identity verification, continuous monitoring, and strict access controls to ensure only authorized users interact with sensitive systems, such as those managing electronic health records that contain personally identifiable information and personal health information. This robust Zero Trust implementation delivers a seamless, secure experience for Veterans in an increasingly interconnected and threat-contested digital environment, while protecting patient safety, ensuring regulatory compliance, and maintaining the public's trust in VA.

It is essential that the Department continues investing in modern cybersecurity tools, skilled personnel, and robust processes. VA's systems hold the personal information and health records of millions of Veterans, and we must protect these systems with the utmost seriousness and commitment they deserve.

Conclusion

In conclusion, every change we are implementing, whether it is enhancing accountability, transforming the workforce, or advancing cybersecurity, is firmly rooted in a singular mission: to deliver unparalleled service to our Veterans. We are not merely modernizing systems; we are constructing a future-ready VA where platforms are secure, teams are empowered, and every dollar generates a significant impact.

I am eager to address your questions and collaborate with you to develop an IT enterprise that truly honors those who have served. Thank you.