ELECTROSOFT NEWSLETTER: Q2 2025

INTRODUCTION

As we look back on the second quarter of 2025, we remain focused on our mission: strengthening cybersecurity and IT services for federal defense and civilian agencies. One of the highlights of the quarter was welcoming Kimberly Esparza as our new Vice President of Human Resources and a key addition to our leadership team.

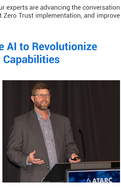
We also continued exploring the growing impact of artificial intelligence on federal cybersecurity, sharing what we're learning with our peers and partners. We were honored and humbled to be recognized on several regional and national award lists — acknowledgment that reflects the dedication of our team and the trust of our customers.

Thank you for being part of our mission-driven journey. Read on for more Q2 highlights.

ADVANCING HR AS KEY PILLAR OF LEADERSHIP AND GROWTH

A respected strategist in the GovCon space, Kimberly Esparza joined Electrosoft as Vice President of Human Resources. She brings the leadership and expertise to help scale our workforce as we grow.

Electrosoft Hires GovCon HR Strategist Kimberly Esparza as VP of Human Resources



Esparza brings more than two decades of federal contracting HR experience, building scalable HR infrastructures, supporting workforce expansion, and fostering high-performance workplaces during periods of rapid growth.

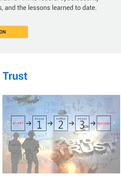
"As we expand our capabilities to support mission-critical government programs, attracting and retaining top talent is essential," said Dr. Sarbari Gupta, CEO of Electrosoft. "Kimberly brings the kind of strategic leadership we need. Her impressive experience building agile, high-performing teams during times of transformation will help us strengthen our workforce and ensure we scale with purpose and efficiency."

READ THE NEWS

SHARING INSIGHTS AND EXPERTISE

Through webinars, tech talks, and new white papers, our experts are advancing the conversation around using AI to modernize SOC operations, support Zero Trust implementation, and improve cyber training outcomes.

Tech Talk | Leveraging Generative AI to Revolutionize Cyber Training and Enhance SOC Capabilities

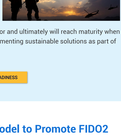


Electrosoft's Vice President of DOD Programs, Jason Ballah, recently delivered an Emerging Technology Talk to federal government and industry leaders at ATARC's Public Sector Cyber AI Convergence Summit in June. The event brought together experts at the intersection of artificial intelligence and cybersecurity.

Jason's educational session, ***"Leveraging Generative AI to Revolutionize Cyber Training and Enhance SOC Analyst Capabilities,"*** focused on two key use cases for applying AI in Security Operations Center (SOC) environments.

WATCH THE VIDEO

Webinar | Harnessing Generative AI: Transforming Federal Cybersecurity Programs



With cyber threats becoming more common and sophisticated, many look to Generative AI as a transformative way to enhance cybersecurity functions, including threat detection, vulnerability management, security operations, and compliance activities. However, as a relatively new technology, Generative AI's benefits and shortcomings are just coming into view.

On April 10, Dr. Sarbari Gupta, Electrosoft's CEO and Founder, joined five other federal cybersecurity experts for a one-hour ATARC educational webinar, **"Harnessing Generative AI: Transforming Federal Cybersecurity Programs."** Electrosoft sponsored the event.

Panelists discussed the challenges of integrating Generative AI into federal cybersecurity initiatives, sharing specific use cases and pilot projects, and the lessons learned to date.

VIEW THE DISCUSSION

White Paper | Implementing Zero Trust

Federal agencies face a mandate to implement a Zero Trust Architecture (ZTA) across their systems and networks. Executive Order 14021 and Office of Management and Budget Circular M-22-09 set forth the specific requirements and established implementation milestones. The transition, however, well delineated, is anything but straightforward. The reason is simple: ZTA is not a technical shift. ZTA requires organizational and process changes within and across agencies.

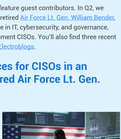
READ MORE INSIGHTS

White Paper | IT Audit Readiness — The Readiness Journey

Both U.S. defense and civilian agencies must undergo independent audits to demonstrate compliance with federal information technology (IT) audit controls. Agencies often struggle to achieve a state of readiness for these audits as a means of minimizing IT findings, improving FIAR compliance, and gaining an understanding of options for remediation of IT findings resulting from the audit. Most organizations start with reactive tactical remediation of deficiencies found by the external auditor and ultimately will reach maturity when they are proactively self-identifying and robustly implementing sustainable solutions as part of normal business operations.

SEE THE JOURNEY TO READINESS

White Paper | Shared Services Model to Promote FIDO2



Given the current cyber threat environment, a straightforward means for multifactor, phishing-resistant authentication is needed. The vulnerabilities associated with traditional passwords are well known and well documented.

Electrosoft, in support of the GSA Office of Governmentwide Policy, has been seeking ways to accelerate Fast Identity Online 2 (FIDO2) adoption within the federal enterprise.

The advantages of a FIDO2/Derived FIDO2 Credential shared services model are many, as this white paper details.

LEARN MORE

RECOGNIZED GOVTECH LEADERSHIP

We're honored to have received several industry recognitions this quarter — and especially proud of those that reflect the voices of our team. Being named a 2025 Washington Post Top Workplace for the fourth year is a meaningful milestone, as it's based entirely on employee feedback. It speaks to the consistency, commitment, and community our team continues to build every day.

Below are three awards we were proud to receive in Q2. You can find a full list of our awards and recognitions on our website.

Virginia Business | Best Women-Owned Business in Virginia

Virginia Business honored Electrosoft as one of its 2025 Best Women-Owned Businesses in Virginia. This award highlights standout companies across the Commonwealth that have demonstrated long-term business success and leadership.

Washington Business Journal | Largest Private Companies in D.C. Area

Washington Business Journal named Electrosoft among its 2025 list of the Largest Private Companies in the greater Washington, D.C. area. This year, the 333 companies on the list generated $186 billion in combined revenue in 2024 and employed more than 417,000 people. Based on 2024 revenue, Electrosoft is ranked #135 on the list.

Washington Post | Top Workplaces 2025

Electrosoft has once again been recognized as a Washington Post Top Workplace for 2025. This is the fourth time that the company has earned a place on the list.

"What makes The Washington Post Top Workplace award so meaningful to me is that it's based entirely on our employees' voices," said Dr. Sarbari Gupta, CEO of Electrosoft. "Team member feedback shapes how we grow as a company — and it's incredibly rewarding to know our people feel supported, respected, and proud to be part of this team."

PERSPECTIVES AND BEST PRACTICES

In addition to insights from our team, we occasionally feature guest contributors. In Q2, we were honored to publish a thoughtful Electroblog from retired Air Force Lt. Gen. William Bender, a member of our Board of Advisors. With deep expertise in IT, cybersecurity, and governance, Bill shares his perspective on best practices for government CISOs. You'll also find three recent blogs from our team below. For even more, explore all Electroblogs.

Securing the Future: Best Practices for CISOs in an Evolving Threat Landscape | Retired Air Force Lt. Gen. William Bender

Federal Chief Information Security Officers (CISOs) operate in an increasingly complex threat landscape. To be effective, they cannot rely on a single cybersecurity approach.

To strengthen cyber resilience, CISOs require a comprehensive approach to agency cybersecurity that starts with the implementation of an "industry-standard" framework to ensure comprehensive data protection measures. They also need to implement a Zero Trust (ZT) Security Model and be proactive in enhancing their organization's security posture by strictly adhering to Secure-by-Design Principles in software development efforts.

KEEP READING

Physical Security and Artificial Intelligence | Seth Berger

Perhaps no concept has been more influential since the invention of computing technology than artificial intelligence (AI). AI has had a significant impact on every industry, as it can automate many tasks that were previously performed by humans.

It is safe to assume that AI will impact physical security as well. I believe AI will only make us safer by making electronic security systems proactive rather than reactive.

DISCOVER MORE

Making the Boss a Success | Peter Martini

“We failed him,” said our Command Sergeant Major when our organization's commander was not selected for promotion. In an instant, I moved from empathy to introspection and began a journey of asking, “Am I responsible for my boss's success, and, if so, how can I help my boss succeed?"

Use case: My boss doesn't have …

Create it! In many cases when something is lacking, it can be drafted for the boss and provided upward. Waiting on a policy decision? Draft a Course of Action paper with options and recommendations. Can't get a meeting with another office? Draft an email for the boss to send to set the ball in motion. Don't let absence prevent action.

READ ON FOR MORE

So Long to P@ssw0rd$ | Sean McGinnis

Traditional password-based systems are often cumbersome, leading to weak password choices and password reuse. Passkeys, by contrast, offer a more user-friendly approach that enhances security and minimizes the risks associated with password breaches. This shift toward “passwordless" authentication reflects a broader movement supported by major technology players including Apple, Google, and Microsoft.

Passkeys rely on device-based authentication and public key cryptography to make it harder for threat actors to exploit vulnerabilities.

LEARN MORE