ELECTROSOFT
NEWSLETTER: H1 2026

INTRODUCTION

April 2026 marked a milestone for Electrosoft: 25 years of partnering with federal agencies to solve their most pressing technology and mission challenges. What began as a cybersecurity and IT services firm has grown, deliberately and steadily, into a leading federal cybersecurity, digital engineering, and intelligent automation company. The shift comes from years of investment in the capabilities our customers need most.

The first half of this year embodied that growth. We strengthened our leadership team to guide the next chapter, advanced mission-critical work for customers across DLA, CISA, NIST, and beyond, and continued sharing the expertise our team brings to the federal community every day. Thank you for being part of this milestone with us. We're just getting started.

MARKING MILESTONES, BUILDING LEADERSHIP

In addition to celebrating our silver anniversary, we welcomed a new COO and promoted a defense leader to the role of Vice President of DoD Programs, deepening the leadership experience and cybersecurity expertise on our executive team. They will help us continue to drive our growth and enhance our defense programs.

Electrosoft Celebrates 25 Years of Federal Cybersecurity Innovation and Impact

Founded in 2001 and led by its founding CEO, Dr. Sarbari Gupta, the company has grown from a small, focused team into a trusted partner on some of the federal government's most consequential cybersecurity and digital engineering programs.

"I founded Electrosoft because I believed federal agencies deserved a cybersecurity partner that would grow with them through every shift in technology and every evolution in the threat environment. Twenty-five years in, that belief has only gotten stronger," said Dr. Gupta. "What fills me with the most pride isn't the milestone itself, but the trust we've built and the team that earned it."

LEARN MORE

Electrosoft Names Former USPTO CIO Jamie Holcombe as COO

Electrosoft appointed Jamie Holcombe as Chief Operating Officer. He brings more than 30 years of federal technology and cybersecurity leadership to the role. Previously, Holcombe served as CIO for the U.S. Patent and Trademark Office, where he led one of the federal government's most significant cloud-first, AI-enabled enterprise modernization efforts.

"The federal market is increasingly seeking integrated cyber, AI and cloud modernization solutions," said Dr. Sarbari Gupta. "Jamie has led exactly that kind of transformation at enterprise scale, and we couldn't be more pleased to welcome him to Electrosoft at this pivotal moment."

MEET JAMIE

Electrosoft Promotes Cecil Dildine to Vice President of DoD Programs

Cecil "Cease" Dildine was promoted to the position of Vice President of DoD programs. A veteran cyber and audit program management executive, Dildine brings more than 40 years in federal service to the role, including two decades as a U.S. Army Counterintelligence Warrant Officer. He will guide Electrosoft's Department of Defense portfolio, providing strategic direction, operational leadership, and collaborative engagement to deliver mission-driven solutions.

READ ABOUT CEASE

ADVANCING FEDERAL CYBER MISSIONS

Electrosoft has secured a series of new contracts while renewing and expanding relationships with trusted customers and partners. We are especially proud to have earned places on the NASA SEWP VI GWAC and the CISA Digital Transformation Support Services BPA, a continuation of expanding our footprint in federal cybersecurity, AI and automation, and digital engineering.

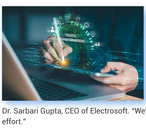
Electrosoft Awarded Positions on NASA SEWP VI in Groups B and C

The government-wide acquisition contract provides federal agencies with streamlined access to IT products and services and carries a 10-year ordering period with a $20 billion ceiling per awardee. This award expands the firm's contract vehicle access for cybersecurity, digital engineering, and AI delivery across the federal enterprise.

"Federal agencies are under pressure to modernize faster and strengthen their security posture, often with fewer resources. SEWP VI gives them a streamlined on-ramp to the capabilities they need most," said Dr. Sarbari Gupta, CEO of Electrosoft.

LEARN MORE

Electrosoft Secures Position on $500M CISA Digital Transformation Support Services BPA



Electrosoft is one of only four awardees on the $500 million Cybersecurity and Infrastructure Security Agency (CISA) Digital Transformation Support Services (DTSS) Blanket Purchase Agreement. The award reinforces the company's leadership in federal cybersecurity, digital engineering, and enterprise AI.

"CISA is a pioneer and continues to lead the way in digital transformation for federal agencies," said Dr. Sarbari Gupta, CEO of Electrosoft. "We're honored to be part of CISA's digital transformation effort."

DISCOVER CISA DTSS

Electrosoft Awarded DLA Contract to Support Systems Engineering IT Modernization

Electrosoft will deliver expanded systems engineering and enterprise data strategy support as DLA accelerates its Digital-Business Transformation initiative across one of the Department of Defense's most complex logistics enterprises.

"The trust DLA has placed in us to continue this work speaks to what our team has delivered, and what we are committed to delivering going forward," said Cecil Dildine, Vice President of DoD Programs at Electrosoft. "I am proud of the dedication and expertise of this group, and we look forward to building on the foundation we have established together."

READ ON

Electrosoft Earns Recompete Award to Advance DLA's G-Invoicing Modernization

DLA's G-Invoicing effort supports federal requirements for reimbursable work with Department of Defense and civilian trading partners, spanning both Order to Cash and Procure to Pay processes. The agency has already deployed significant capabilities, with additional work ahead to expand coverage across remaining transaction types.

Building on a successful implementation, Electrosoft will support automation and audit readiness advancements. "This recompete award is a direct reflection of the trusted partnership we have built with DLA and our shared commitment to advancing mission-critical financial modernization," said Cecil Dildine, Vice President of DoD Programs at Electrosoft.

DISCOVER MORE

Electrosoft Awarded Follow-On DLA Contract to Advance Defense IT Modernization and Cybersecurity

Under the award from DLA J6, Electrosoft will continue delivering systems security engineering and technical support to advance the Information Technology (IT) modernization and cybersecurity of DLA's critical defense infrastructure.

"As threats to defense IT infrastructure evolve, our focus remains on delivering the engineering rigor and cybersecurity expertise federal agencies need to protect the systems that keep our nation's defense supply chain running," said Dr. Sarbari Gupta, CEO of Electrosoft. "We are honored to continue this important work with DLA."

READ MORE DETAILS

Electrosoft Awarded Follow-On Task Order for NIST Cryptographic Validation Program Support

NIST's Cryptographic Validation Program plays a vital role in the security of both government and commercial technology. Products certified under the program are cleared for handling sensitive information across federal agencies and regulated industries, including financial services and healthcare, making the program's integrity essential to a broad swath of the U.S. economy.

This award extends Electrosoft's two-decade partnership supporting the nation's cybersecurity standards infrastructure. Under this contract, Electrosoft will deliver ongoing operational and development support to the program that certifies cryptographic products for use across the U.S. government and regulated industries.

LEARN MORE

SHARING AI AND CYBERSECURITY INSIGHTS

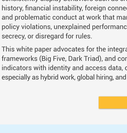
Through white papers, interviews, and educational webinars, we are eager to share our stories, lessons learned, and insights on shared technology challenges and best practices, innovative solutions, and leadership reflections. You're invited to browse through these publications from 2026 (so far).

White Paper: Comprehensive Analysis of Cybercriminal Behavior Throughout the Intrusion Lifecycle By Kirk Lurie

This white paper offers actionable insights for cybersecurity practitioners. By integrating behavioral analysis with frameworks such as MITRE ATT&CK and the Cyber Kill Chain/Unified Kill Chain, the new resource maps adversary tactics and techniques throughout the full intrusion lifecycle. Real-world case studies, including SolarWinds, Colonial Pipeline, Equifax, MOVEit/CLOP mass extortion, and Microsoft Exchange/Hafnium, illustrate how these behavioral patterns manifest, underscoring the urgency of proactive defense strategies.

DOWNLOAD

White Paper: Balancing Security and Usability — Integrating Identity, Credential, and Access Management and Segregation of Duties in a Zero Trust Framework By Mythili Arun



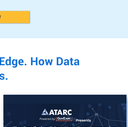
As government and enterprise environments accelerate adoption of ZTA, the intersection of ICAM and SoD is becoming increasingly critical.

ICAM ensures users are accurately identified, authenticated, and appropriately authorized, while SoD is a risk management control that thwarts fraud by preventing any single individual from controlling multiple stages of a critical process. Although both domains reinforce the Zero Trust principle of least privilege, organizations often struggle to implement SoD without degrading usability or creating operational friction. This white paper explores how ICAM and SoD can be integrated to achieve a balanced, secure, and efficient operating environment, supported by leading public sector and industry standards.

READ MORE

White Paper: Behavioral Signs of Insider Threats By Kirk Lurie

Traditional approaches for identifying and mitigating insider threats often identify a breach after the fact. Effective security requires early recognition of warning signs often manifested in behavioral patterns. Individuals who commit insider threats consistently display behaviors such as criminal history, financial instability, foreign connections, and problematic conduct at work that manifests as policy violations, unexplained performance changes, secrecy, or disregard for rules.



This white paper advocates for the integration of behavioral science, personality assessment frameworks (Big Five, Dark Triad), and continuous monitoring. By combining behavioral indicators with identity and access data, organizations can detect risks before escalation, especially as hybrid work, global hiring, and AI-driven impersonation broaden the threat landscape.

DOWNLOAD

Authority Magazine: Sarbari Gupta Of Electrosoft On Pushing the Boundaries of AI

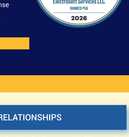
In this interview with Authority Magazine, Dr. Sarbari Gupta shares how artificial intelligence first captured her interest and inspired her to integrate AI into Electrosoft's cybersecurity solutions. To advance this vision, she established a Technology and Innovation Directorate focused on accelerating AI-driven innovation at the firm. Later, she accepted a strategic investment from DigitalNet.ai to further scale and modernize cyber defense by leveraging their groundbreaking AI solutions and service offerings.

While AI holds tremendous promise, Dr. Gupta emphasizes that its adoption must be thoughtfully and responsibly managed. She highlights five critical considerations for expanding AI use: Governance, Provenance, Data, Human Element, and Fallibility. Her selection of these key factors is illustrated through compelling real-world examples.

READ INTERVIEW

ATARC Webinar: The Predictive Edge. How Data Integration Transforms Logistics.

Electrosoft's Enterprise Technology Solutions Manager, Travis Cutts, joined three other federal experts for a one-hour ATARC educational webinar, "The Predictive Edge: How Data Integration Transforms Logistics." Electrosoft sponsored the event.



This session explored how real-time data, APIs, and AI/ML models are enhancing logistics by forecasting delivery times, optimizing routes, and predicting disruptions. It also highlighted how Predictive Logistics and integrated data ecosystems are shifting supply chains from reactive to proactive, supporting mission readiness through advanced data strategies and Zero Trust methodologies.

WATCH VIDEO

Mergermarket: Electrosoft Services eyes AI-driven growth after DigitalNet.ai investment

After years of cautious exploration, government organizations are increasingly prioritizing practical AI adoption to strengthen cybersecurity, streamline operations, and support Zero Trust architectures. In this interview, Electrosoft CEO Dr. Sarbari Gupta discussed the company's strategic investment and how Electrosoft is leveraging its deep federal expertise to help agencies introduce automation and AI capabilities in secure, mission-critical environments.

"The shift in how federal agencies are approaching AI has been significant," said Dr. Sarbari Gupta, CEO of Electrosoft. "Our customers are moving beyond AI curiosity and starting to ask for AI solutions that improve security, efficiency, and mission outcomes. Our partnership with DigitalNet ai positions us well to meet that demand while staying grounded in trust and compliance."

LEARN MORE

EARNING INDUSTRY RECOGNITION

We're always proud to earn industry awards for company milestones and trends. In the first half of this year, we were recognized as a top technology GovCon in the market and, based solely on employee feedback, as a Top Workplace in the Greater Washington area.

Electrosoft Named a 2026 Top Workplace by WTOP News, Marking Five Years on the List

The Top Workplaces award is based solely on employee feedback gathered through a confidential survey administered by a third party. The survey measures employee experience across a range of themes, including whether employees feel respected and supported, enabled to grow, and empowered to execute.

Dr. Sarbari Gupta shared, "I'm proud of our team, and grateful to everyone who took the time to share their voice in this survey."

SEE MORE

Electrosoft Climbs to #56 on WBJ's List of Largest GovTech Contractors in Greater Washington

Electrosoft has been ranked #56 on the Washington Business Journal's 2026 list of the largest government technology contractors in the Greater Washington region, rising 10 spots from last year's #66 ranking. The move reflects the company's continued growth, expanding role in the federal market, and success in delivering high-impact technology and cybersecurity solutions that help defense and civilian agencies meet evolving mission demands.

READ ON

GIVING BACK, BUILDING RELATIONSHIPS

As much as our team is inspired by the work we do together, we also love opportunities to gather to celebrate special milestones and to give back through our time, talent, and treasure. Here are two special events we've enjoyed this year.

Electrosoft Participates in The Arc's Community Challenge for 8th Consecutive Year

On Saturday, June 6, 2026, Team Electrosoft joined other companies, community organizations, families, and supporters for The Arc of Northern Virginia's annual Community Challenge. The event raises funds to support the organization's programs, services, and advocacy for people with intellectual and developmental disabilities. It was the eighth consecutive year that Electrosoft sponsored a team.

SEE THE TEAM

DLA America 250 Celebration

It was a true honor to join the Defense Logistics Agency for their "DLA Celebrates America 250!" ball in Ft. Belvoir. At this evening of connections and celebration, our team was especially delighted to hear from the guest speaker, Dr. William Shane Story, Command Historian, U.S. Army Materiel Command (AMC). He brought the history of military logistics to life, leaving the whole room inspired by what so many accomplished in years past and how the Defense Logistics Agency supports today's modern missions.

SHARING EMPLOYEE EXPERTISE

We're proud to share a sample of Electroblogs from team members across our company. AI and automation, vulnerability management, FISCAM, and innovation are all "hot topics" from the first half of this year. We invite you to browse these and other cybersecurity and digital transformation insights on our website.

Closing the Gaps in Continuous Monitoring By Lindsay Bloom

Safeguarding information networks is an ongoing, evolving challenge. Continuous monitoring ensures that analysts and stakeholders know the risks, mitigations, and status of their infrastructure while keeping critical data reliable and secure.

Vulnerability Management (VM) and Identity and Access Management (IAM) are central to cyber defense. VM focuses on proactively identifying and remediating weaknesses, while IAM ensures that the user base and non-user entities (servers and applications) are protected from malicious actors, privilege escalation, and insider threats.

KEEP READING

Automation vs. Artificial Intelligence: What's the Difference? By Jeanne Zepp

People often use the terms automation and artificial intelligence interchangeably. Both seem to perform similar actions: speed up work, reduce human effort, and improve output consistency. Yet the two concepts couldn't be more different.

Understanding where automation ends and AI begins isn't just a nice-to-know concept. Organizations making decisions about technology investments, staffing, and long-term strategies for digital transformation must understand the differences today.

READ MORE

Recursive Self-Improvement in AI: What Is It? By Jeanne Zepp

Recursive self improvement (RSI) is a theoretical concept that describes an artificial intelligence (AI) system's capability to improve itself while simultaneously improving its capacity to make further improvements. In this model, enhancement is not a one time upgrade but a continuous feedback loop.

The idea of incremental optimization is not new. Popular culture has explored variations of it for decades in films such as The Matrix and The Terminator. What distinguishes RSI from ordinary optimization, however, is its recursive nature. As AI systems become more capable, RSI provides a mechanism by which speculative fiction could become reality.

READ ON

Proactive Vulnerability Management: Why NVD and CVE Analysis Can't Wait By Kirk Lurie

Two publicly available resources — the National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVE) — catalog known security vulnerabilities in software and hardware. Proactive analysis allows security teams to understand what vulnerabilities exist in their deployed systems, how they could be exploited, and ultimately, to prioritize mitigation efforts before attackers capitalize on them.

LEARN MORE

FISCAM 2024: Interpreting Controls for Sustained Compliance By Michael Ball

Federal agencies and contractors rely on established audit frameworks to ensure the integrity and security of their information systems. One of the most important is the Federal Information System Controls Audit Manual (FISCAM), which was updated in 2024 for the first time in more than a decade.

Like many standards and frameworks, FISCAM is built on core guidelines, with the National Institute of Standards and Technology Special Publication (NIST SP) 800-53 serving as the widely recognized foundation for most government agencies. Several updates to NIST SP 800-53 (now in Revision 5) triggered a ripple effect across compliance frameworks and processes. As a result, the long-standing FISCAM 2009 guidance has now been updated to FISCAM 2024.

READ MORE

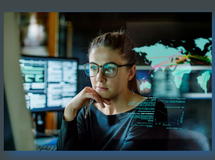
Innovation: The Key to Continuing Success By Cecil Dildine

Integrity, Customer Service, Excellence, Innovation, and Respect are Electrosoft's core values. Innovation, which is crucial to continuing success, is usually associated with a new method, idea, or product. Innovation challenges the old way of doing things. It involves thinking outside the box and looking at problems from different perspectives.

Innovation can be disruptive or incremental, and it can take many forms. Would-be innovators can look for gaps (what's broken), explore future needs, or investigate better ways of doing things. Innovation should include ways to integrate automation tools to save time and reduce errors.

KEEP READING

XDR and SIEM: An Alphabet Soup that Takes Cybersecurity to New Levels By Jeanne Zepp



Security Operations Centers (SOCs) exist to detect and mitigate cyber threats. The sheer scope of data, systems, and devices that analysts must monitor — and the decisioning involved in determining whether a true threat exists — is creating an essential need for technology such as XDR and SIEM.

LEARN MORE

Thank you for your continued partnership. We're delighted to be advancing the cybersecurity resilience of the federal government and ensuring mission success, together.