ELECTROSOFT
NEWSLETTER: Q3 2022

INTRODUCTION

In a recent interview, our CEO, Dr. Sarbari Gupta, was asked to reflect on the early days of her career. She talked about discovering computer security and cryptography 30 years ago and deciding to focus on computer and data security.

> "I have never looked back," she commented. "The Internet and World Wide Web have completely changed our world over the last three decades, yet as change progresses, the field only grows in relevance."

That reflection could also sum up what we experienced in the third quarter of 2022: a growing need for evolving cybersecurity solutions. We're pleased and proud that federal defense and civilian organizations continue to entrust Electrosoft to support their cybersecurity and resilience, including three client contracts totaling $39.2 million.

Additionally, we continue to engage in conversations with clients, partners and standards bodies to shape our latest thinking, actions and thought leadership. We invite you to learn more about these highlights, below.

Electrosoft Awarded Three Contracts Totaling $39.2M for Federal Cybersecurity and Resilience Support

We are proud to announce that, in Q3 2022, Electrosoft earned three major contracts for federal civilian and defense cybersecurity and resilience support.

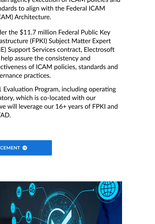
The awards from the U.S. Transportation Command (USTRANSCOM), General Services Administration (GSA) and Defense Logistics Agency (DLA) totaled $39.2 million.

USTRANSCOM Selected Electrosoft for $21M SISO Support Services Contract

USTRANSCOM is a critical combatant command that provides elite, full-spectrum global mobility and logistics support to the 10 other U.S. combatant commands, the military services, defense agencies and other government organizations.

Enabled by various information technology, operational technology, platform IT and cyber-physical systems, the command conducts delivery operations of mission-essential people, goods and services to protect and sustain warfighters around the world.

Under the $21M USTRANSCOM Senior Information Security Officer Support Services contract, Electrosoft will provide a range of IT services to support cyber resilience for USTRANSCOM's specialized technology and logistics mission environment at Scott Air Force Base.



READ THE FULL ANNOUNCEMENT

GSA Office of Government-wide Policy (OGP), Identity Assurance and Trusted Access Division (IATAD) Awarded Electrosoft a $11.7M Prime Contract

The IATAD coordinates the government-wide civilian agency execution of ICAM policies and standards to align with the Federal ICAM (FICAM) Architecture.

Under the $11.7 million Federal Public Key Infrastructure (FPKI) Subject Matter Expert (SME) Support Services contract, Electrosoft will help assure the consistency and effectiveness of ICAM policies, standards and governance practices.

Among other tasks, our team will support the FIPS 201 Evaluation Program, including operating the Physical Access Control Systems (PACS) test laboratory, which is co-located with our headquarters in Reston, Virginia. Under this contract, we will leverage our 16+ years of FPKI and ICAM thought leadership to support the GSA OGP IATAD.

READ THE FULL ANNOUNCEMENT

Electrosoft Wins $6.5M Defense Logistics Agency AGA Audit Support Contract for Financial and IT System Audit Readiness

Under the $6.5 million DLA AGA Audit Support contract, Electrosoft will deliver a range of IT and professional services to support enterprise segregation of duties (SoD) auditing for financially relevant applications. We will also support the DLA AGA team with internal audit requirements.

Building on our success with government financial and IT system audit and audit readiness, our team will support the Annual Statement of Assurance risk assessment process, conduct quarterly system reviews and support the preparation of the financial statement audit in accordance with applicable government and defense standards and frameworks.

READ THE FULL ANNOUNCEMENT

IN THE NEWS & COMMUNITY

Cybersecurity Thought Leadership From Our CEO

At Electrosoft, we are continually monitoring cybersecurity threats and hazards and evolving our approaches, best practices and solutions to better serve our federal customers and the broader government community.

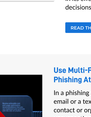
Our CEO, Dr. Sarbari Gupta, shared her insights on supply chain security, benefits and concerns related to Fast Identity Online (FIDO) passkeys and federal agency "bot" security considerations in these recent articles.

Authority Magazine

Sarbari Gupta Of Electrosoft Services On What We Must Do To Create Nationally Secure And Resilient Supply Chains

Authority Magazine

READ FULL ARTICLE



Can FIDO Passkeys and Accountability Coexist?

Security Boulevard

READ FULL ARTICLE

Are Your Agency Bots Up to No Good?

Enterprise Viewpoint

READ FULL ARTICLE

Technology Report: Security Operations Center (SOC)

TECHNOLOGY REPORT: SECURITY OPERATIONS CENTER (SOC)

Today's Security Operations Center (SOC) is not so much a place (physical locale) but rather a functional team (experienced professionals) providing a service (cybersecurity) that can be delivered from any locale.

It is a highly specialized operation staffed by IT specialists with information security backgrounds and dedicated to threat detection, endpoint protection, compliance management and data loss prevention.

Electrosoft's new seven-page Technology Report: Security Operations Center (SOC) steps through the need for management support when creating a SOC, key success metrics, considerations for federal SOC outsourcing and more. It includes an outline of core capabilities and tools of modern SOCs.

DOWNLOAD THE TECHNOLOGY REPORT

ADDITIONAL RESOURCES

Insights from the Electrosoft Team

We're proud to share just a sampling of our Q3 Electroblogs from team members across our company. Read more for perspectives on ransomware, phishing attacks and the human factor as an essential consideration for IT governance.

Recognizing the Human Factor in IT Governance | September 2022

Individual organizations can expend untold millions on IT and information security, but the human factor can be the undoing of even the most sophisticated – and expensive – tools and technology acquired within the most rigorous governance framework.

As concern over information security deepens, it's time that IT governance places great weight on the human element in its effectiveness and efficiency decisions.

READ THE FULL BLOG

Use Multi-Factor Authentication to Foil Phishing Attacks | August 2022

In a phishing attack, the perpetrator sends an email or a text pretending to be a trusted contact or organization. When an unsuspecting victim provides log-in credentials, the attacker then logs into a real website, often causing extensive financial harm.

Industry and government agree ... multi-factor authentication (MFA) can help to thwart phishing attacks.

READ THE FULL BLOG

To Pay or Not To Pay ... Is That the Ransomware Question? | July 2022

Who is protecting the online user? The answer is no one. In fact, most IT environments consider users to be liabilities, not assets deserving protection.

They are seen as the weakest links in the cybersecurity protection scheme. Why? Users browse unsafe websites, open emails with embedded malware or click on links in messages.

READ THE FULL BLOG