ELECTROSOFT

NEWSLETTER: Q1 2023

INTRODUCTION

For more than 20 years, Electrosoft has been supporting the development and update of information assurance and cybersecurity standards as well as special publications designed to better protect federal information, privacy and assets. In that time, the world has changed dramatically. With the emergence and evolution of a digitally interconnected world, cyber adversaries have emerged and evolved to exploit digital vulnerabilities across an increasingly vast attack surface.

The push toward cyber resilience remains an urgent matter. Much of Electrosoft's activity in the first quarter of 2023 reflects our commitment to engage with clients and others in the federal IT services and cybersecurity industry to shape solutions and best practices.

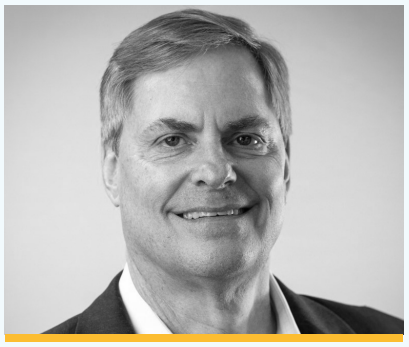
We invite you to learn more about recent additions to our leadership team, cybersecurity industry engagement and thought leadership, below.

Executive Talent: Two Business Development Leaders Join Electrosoft

Building on a year with record-high revenue, Electrosoft added two business development leaders in the first quarter of 2023. Retired Army Chief Warrant Officer Wes Postol was hired as Electrosoft's new Senior Vice President of Business Development. Wes is an award-winning growth executive with more than 30 years of experience driving federal cybersecurity strategy and development and has “a keen ability” to build and lead high-performing teams. Wes is joined by Jeff Wilson, who brings 30 years of business development experience with IT services and consulting companies to his Director of Business Development role at Electrosoft.

WES POSTOL
Senior Vice President of
Business Development

READ MORE



JEFF WILSON
Director of
Business Development

READ MORE

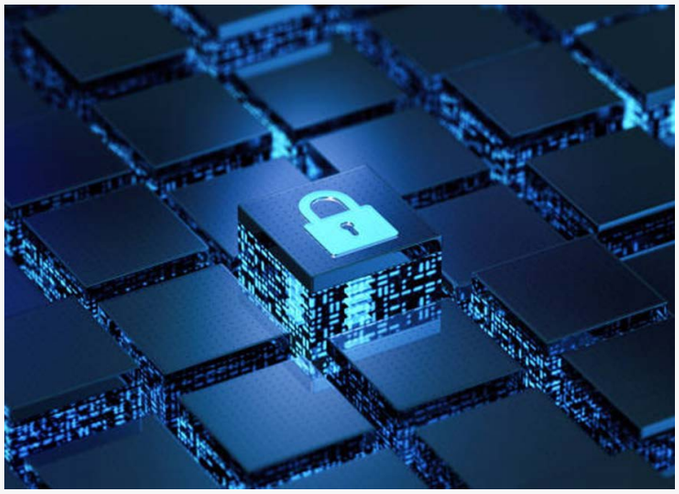
Cybersecurity Industry Engagement: NIST Collaboration and Contract Award

Technology continues to alter the digital landscape and, with it, cyber vulnerabilities and adversary threats, technologies and procedures. In keeping with its responsibility for developing and maintaining information security standards and guidelines, the National Institute of Standards and Technology (NIST) is simultaneously in process of:

- Updating its Digital Identity Guidelines
- Advancing its Cybersecurity Framework
- Reconciling some Special Publications to support revised standards

We are proudly supporting each of these initiatives, helping to increase the cybersecurity of federal agencies and the national information infrastructure.

Dr. Sarbari Gupta, Electrosoft CEO and a NIST Collaborator, Offers Insights on the “Digital Identity Guidelines” Draft Revision



In December 2022, NIST issued for public comment a significant draft revision of its Special Publication (SP) 800-63 “Digital Identity Guidelines,” which was last updated in 2017. Development of the initial public draft was an intensive undertaking. It reflects the cumulative effort of all who worked on NIST SP 800-63 iterations in the past as well as the eight collaborators on the current revision, including Electrosoft's Dr. Gupta and Diana Proud-Madruga.

In March, Dr. Gupta published her insights on the Digital Identity Guidelines and the comments NIST hoped to receive from the public. In addition to feedback on the technical requirements for federal agencies implementing digital identity services, NIST expressed a need to advance equity and address topics of optionality and consumer choice, among others.

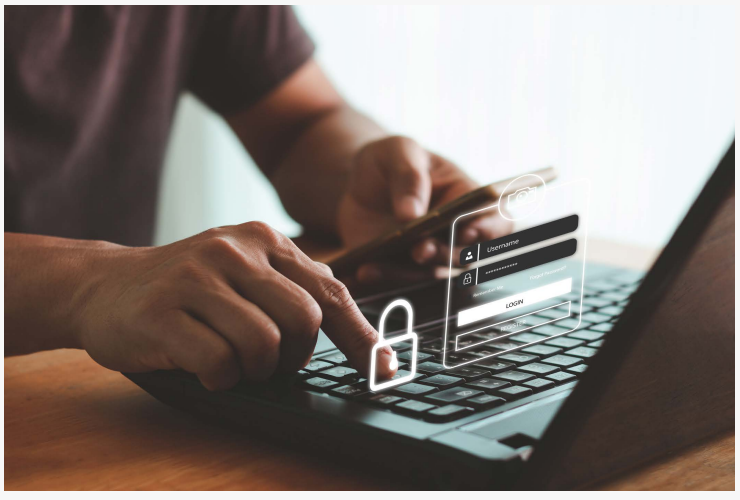
READ DR. GUPTA’S INSIGHTS

Electrosoft CEO Dr. Sarbari Gupta Facilitated NIST Cybersecurity Framework (CSF) 2.0 Workshop

NIST is currently moving through a collaborative process to update its Cybersecurity Framework. As part of the process, NIST hosted an in-person “Journey to the NIST Cybersecurity Framework (CSF) 2.0" workshop on February 22 and 23, 2023, to seek inputs from the community on potential CSF updates. The working sessions covered six parallel tracks, including Assessment and Measurement, which examines potential changes to the CSF to address the assessment of cybersecurity risk management, as well as additional guidance on CSF Tiers. Electrosoft's CEO, Dr. Sarbari Gupta, served as a facilitator for the Assessment and Measurement track during the two-day workshop.

READ ABOUT CSF 2.0 AND THE WORKSHOP

NIST Awards Electrosoft a Prime Contract to Support FIPS 201-3 Special Publication Updates



In Q1 2023, NIST awarded Electrosoft a prime contract to update some Special Publications that support the recently revised Federal Information Processing Standard 201-3. Electrosoft will collaborate and provide technical engineering and standards updates.

“As federal ICAM standards and best practices evolve, it's essential to keep related requirements aligned,” said Dr. Sarbari Gupta, Electrosoft CEO. “We're proud to be a thought leader in government-wide interoperability standards for identity credentials and we're pleased to continue supporting NIST in increasing the security of federal agencies and the National Information Infrastructure.”

READ THE NEWS STORY

Commitment to Quality: ISO 9001:2015

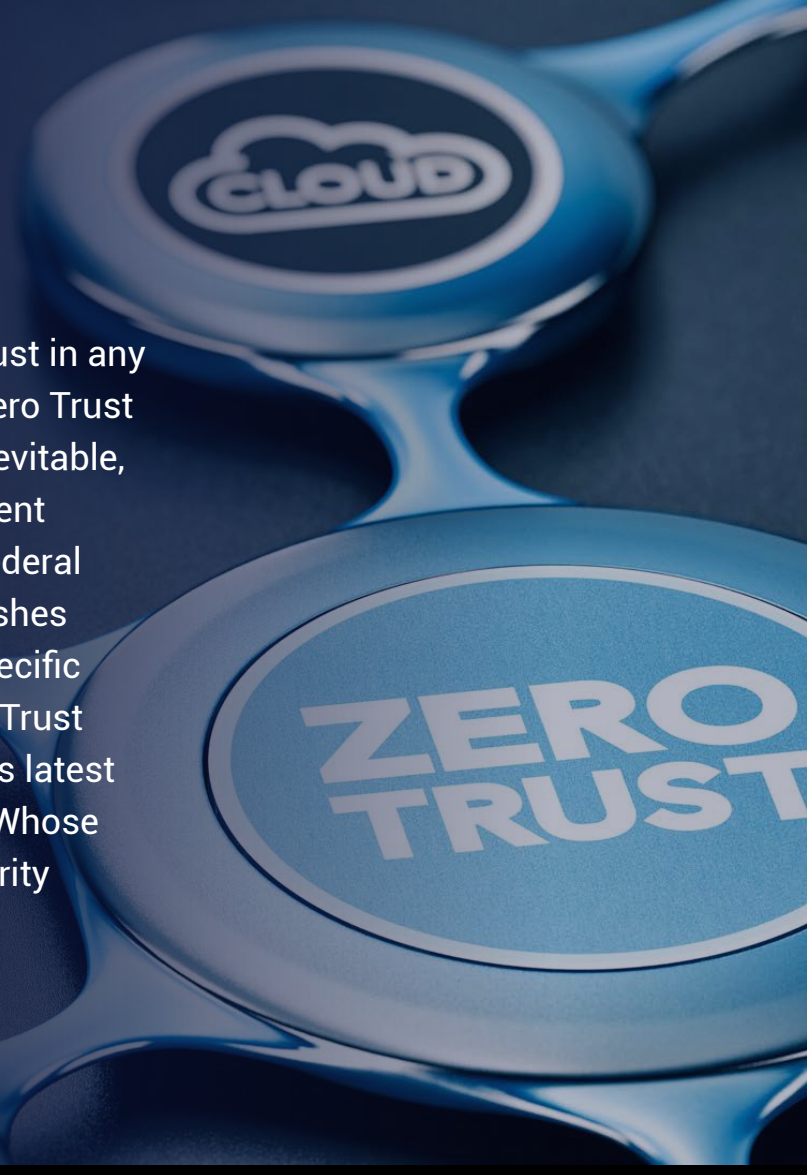
Compliance

Electrosoft successfully completed an annual surveillance audit, continuing the company's 15+ years of compliance with ISO 9001:2015 Quality Management Systems. Successful registration under the International Organization for Standardization standard demonstrates Electrosoft's ability to consistently provide products and services that meet customer and regulatory requirements, as well as to provide enhanced customer satisfaction.

"Excellence drives everything we do. Our passion for delivering consistent, high-value results to our customers drove us to implement a comprehensive QMS for product delivery, operations and management processes," said Dr. Sarbari Gupta, CEO of Electrosoft. "I'm proud that we achieved our initial ISO 9001:2015 certification in 2008 — and have maintained compliance ever since."

READ THE ANNOUNCEMENT

White Paper:
Zero Trust Architecture Thought Leadership

Foundational to the concept of Zero Trust is placing no trust in any user or any element of the IT infrastructure. In addition, Zero Trust operates from the premise that unauthorized access is inevitable, perhaps having already occurred. The Office of Management and Budget Memorandum 22-09 outlines a strategy for federal agency migration to a Zero Trust Architecture and establishes an implementation deadline of September 30, 2024 for specific goals and objectives. The bold federal move toward Zero-Trust Architecture is at once novel and challenging. Electrosoft's latest white paper, Zero-Trust Architecture: A Security Strategy Whose Time Has Come, discusses key features of this cybersecurity strategy based on a review of implementing documents.

DOWNLOAD THE ZTA WHITE PAPER