Electrosoft

Results That Drive Mission Success!

Advancing Zero Trust in Federal ICAM – From Static MFA to Continuous Authentication

Dr. Nnamdi Osia, CCZT
ICAM SME, Electrosoft

Identity Week USA 2025
Washington, DC
September 11, 2025

Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
Fax: (703) 437-9452

Agenda

- Introduction
- Static Multi-Factor Authentication (MFA)
- MFA Policy Drivers
- From Static MFA to Continuous Authentication
- Best Practices and Implementation Approaches
- Wrap-Up

Electrosoft

Introduction

Electrosoft

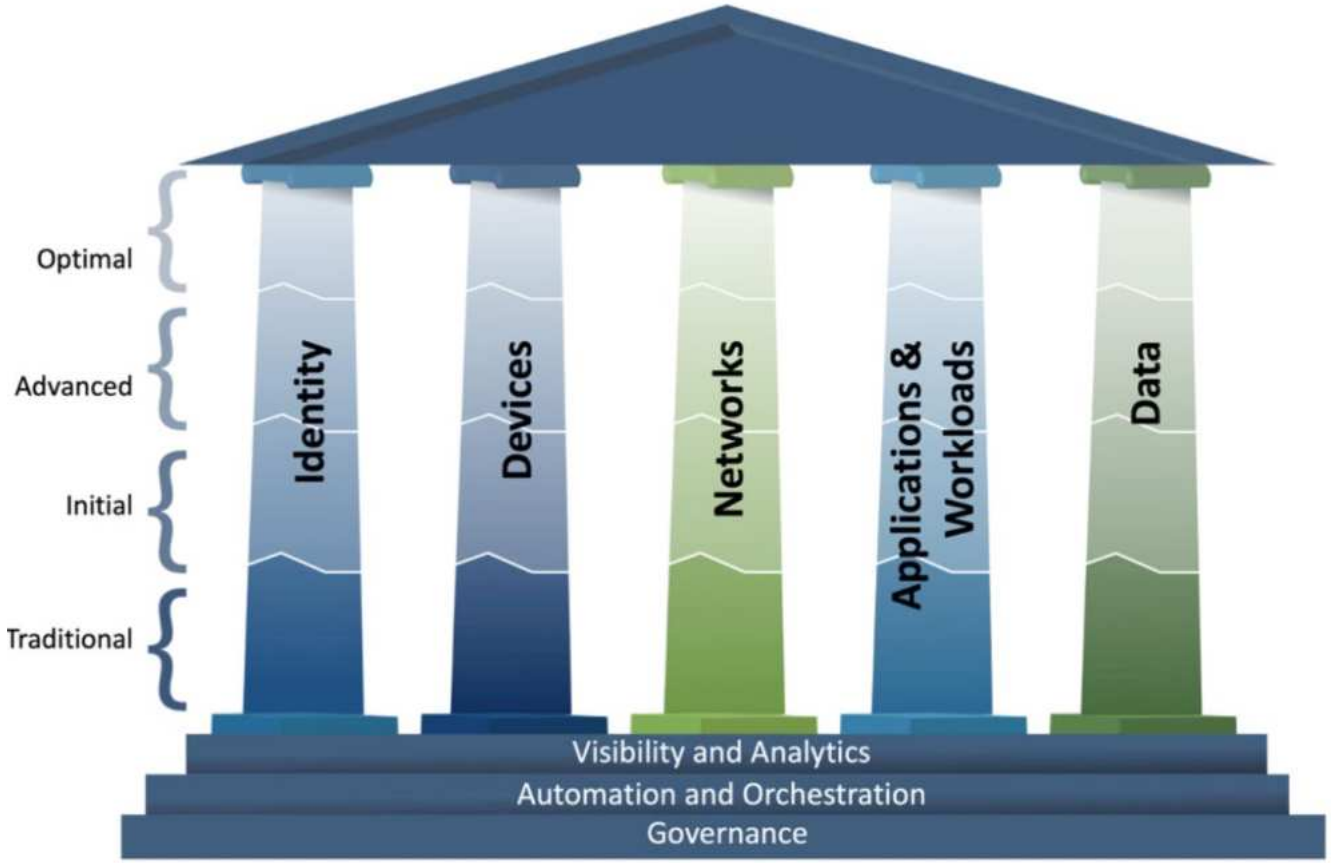
Zero Trust – The Big Picture

- **Problem**
  - Cyber threats are evolving faster than traditional perimeter defenses (e.g., firewalls, VPNs)
- **Solution**
  - Zero Trust Framework
- **Core Tenets**
  - Never trust, always verify
  - Assume breach
  - Least privilege access
  - Continuous verification
  - Policy-driven access decisions

Electrosoft

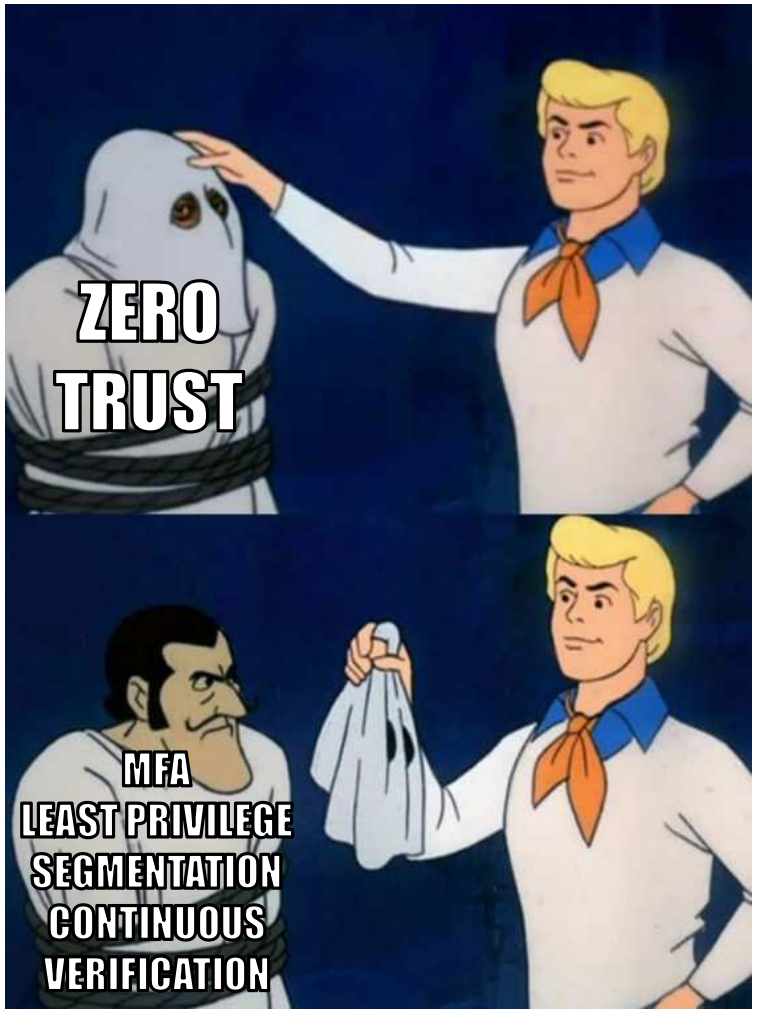
Zero Trust Framework

- **Federal Guidance**
  - OMB M-22-09
  - CISA ZT Maturity Model
  - NIST 800-63-4
- **ICAM as a Foundation**
  - Federal agencies advance Zero Trust via ICAM implementation
- **Identity is the New Perimeter**
  - Access decisions are about *who* (identity) and *context* (location/device)
  - Strong Identity Assurance is foundational for Zero Trust



Electrosoft

Core Security Principles of Zero Trust



- **Multi-Factor Authentication (MFA)**
  - Foundation for strong Identity Assurance using two or more factors
- **Least Privilege Access**
  - Grant only the minimum access required
- **Network Segmentation**
  - Limit lateral movement and isolate sensitive resources
- **Continuous Verification**
  - Trust is never implied; validate users, devices, and sessions in real-time

➡ *This presentation will focus on MFA and how agencies can evolve towards risk-based and continuous authentication within Federal ICAM programs*

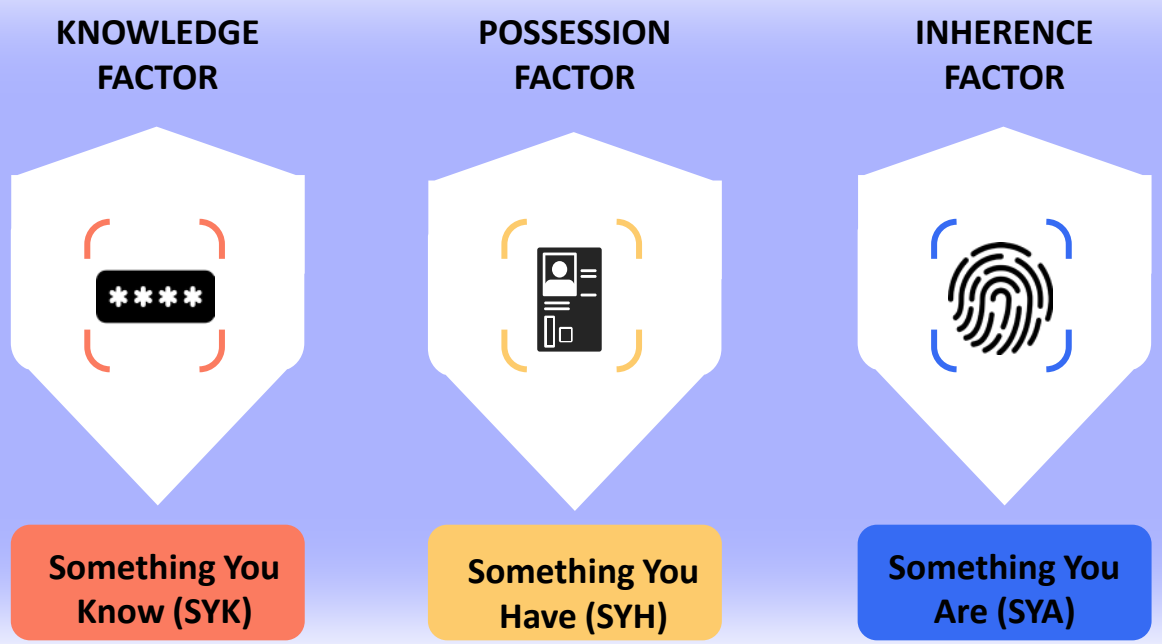
Electrosoft

Static Multi-Factor Authentication (MFA)

Electrosoft

Traditional MFA Approaches

- MFA is the use of two or more factors (e.g., SYK, SYH, SYA)
- With Static MFA, authentication only happens once at login
- Access granted for the entire session without re-evaluation



Electrosoft

Gaps in Addressing Evolving Risks

- **No Continuous Monitoring**
  - Authentication only happens once, and there is no monitoring after access granted
- **Blind to Context**
  - Unable to adapt to risk factors such as device, location, or user behavior
- **Risk of Compromise**
  - Valid MFA token can be stolen/reused

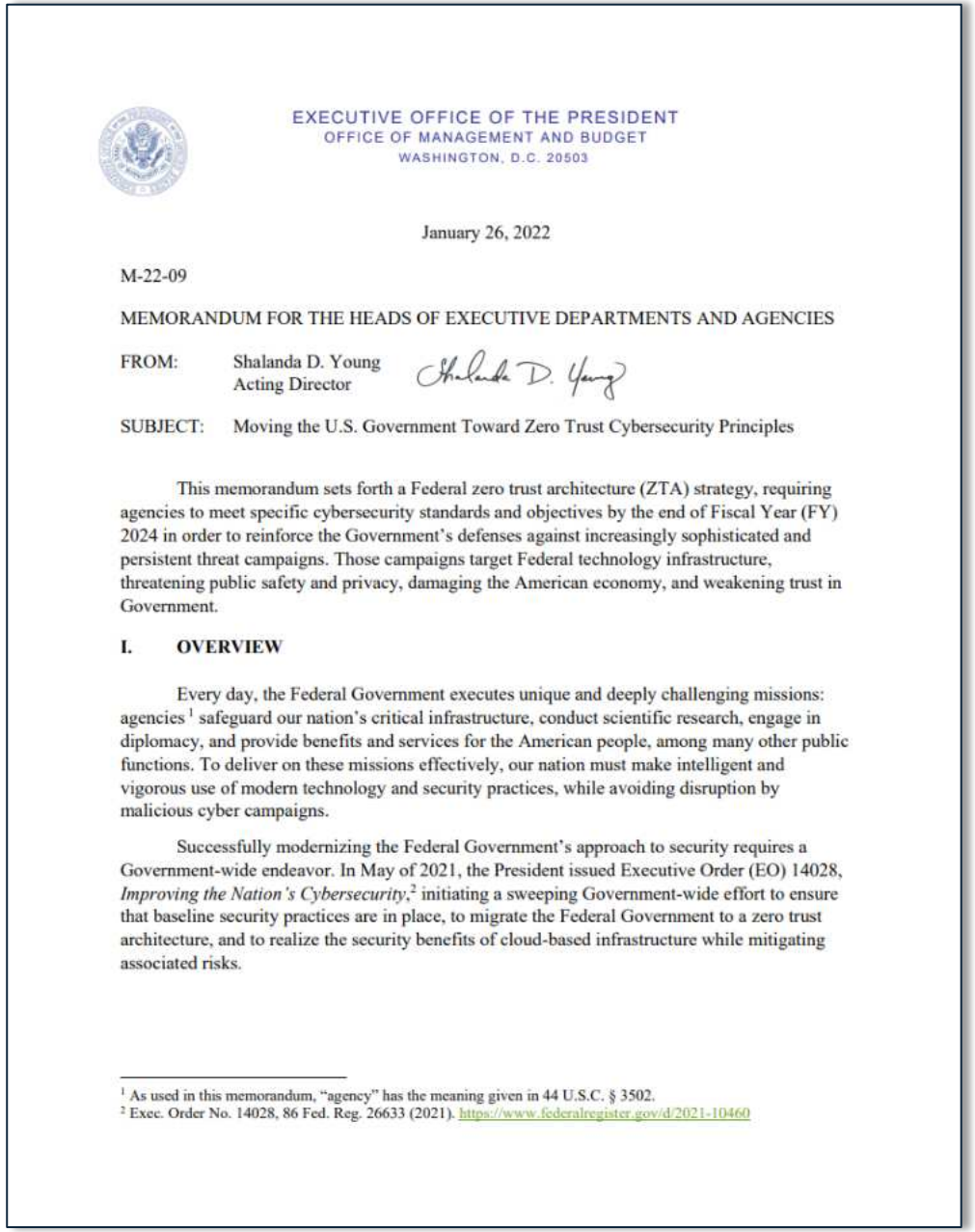
Electrosoft

MFA Policy Drivers

Electrosoft

OMB M-22-09

- **MFA Across Devices**
  - Federal staff must use MFA for access
  - Applies to GFE and non-GFE
- **Phishing-Resistant MFA**
  - Prioritize phishing-resistant methods (e.g., PIV, FIDO2/Web Authn)
  - Passwords + OTPs not sufficient
- **Coverage Across All Systems**
  - On-prem, cloud, SaaS, and privileged accounts
  - No exceptions for legacy or “low-risk” systems



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government’s defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

Every day, the Federal Government executes unique and deeply challenging missions: agencies [1] safeguard our nation’s critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

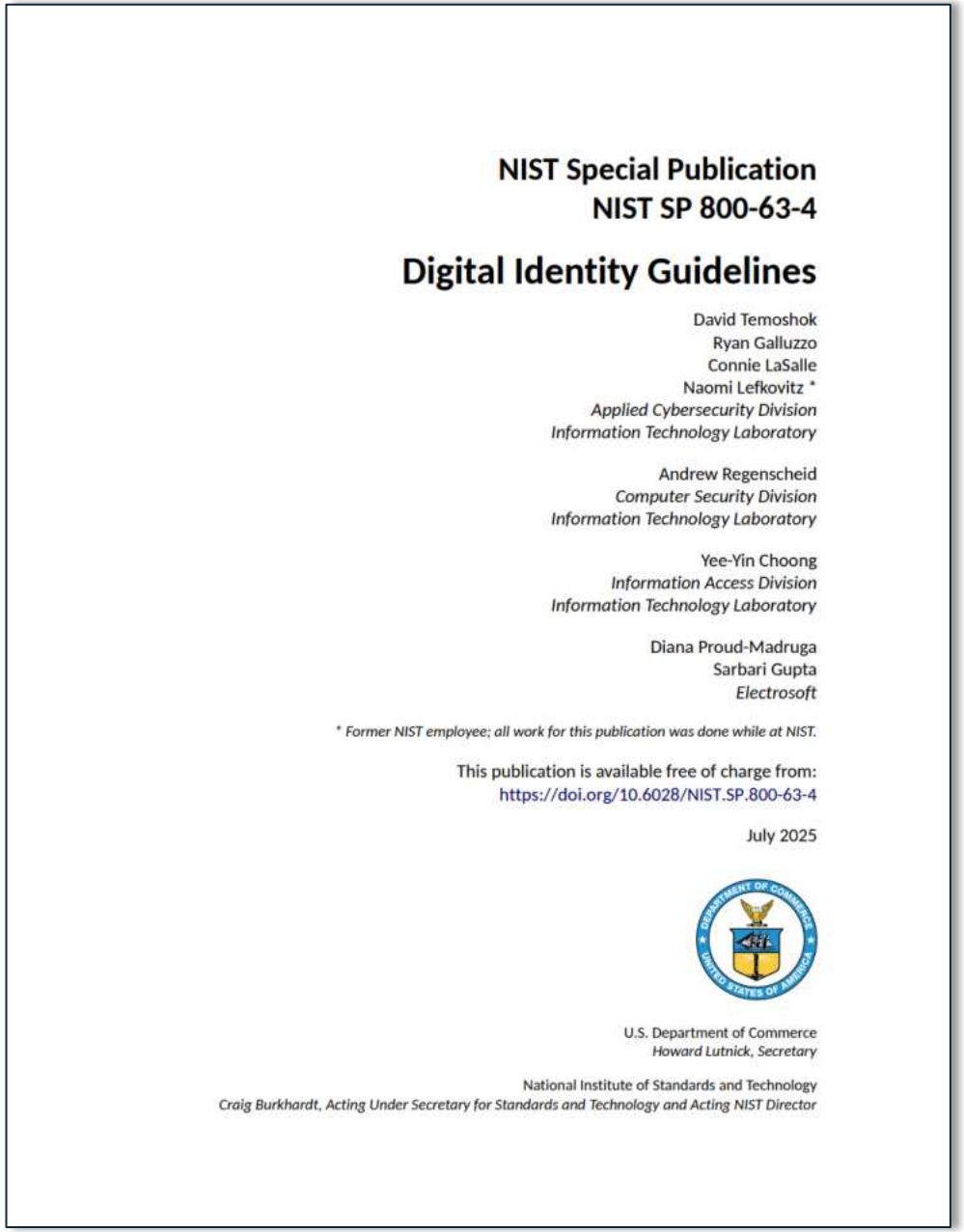
Successfully modernizing the Federal Government’s approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation’s Cybersecurity*,[2] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

[1] As used in this memorandum, “agency” has the meaning given in 44 U.S.C. § 3502.
[2] Exec. Order No. 14028, 86 Fed. Reg. 26633 (2021). https://www.federalregister.gov/d/2021-10460

Electrosoft

NIST SP 800-63-4

- **Authentication Assurance Levels (AALs)**
  - AAL1 – Single-factor allowed (not MFA)
  - AAL2 – MFA required, with at least 2 different factors
  - AAL3 – Requires hardware-based authenticator and additional authenticators such as verifier impersonation resistance
- **Session Management & Reauthentication**
  - Reauthentication required at intervals, or when risk changes
  - Strong binding of sessions to authenticator used at login
- **MFA Factor Types (SYK, SYH, SYA)**
- **Phishing Resistance**



NIST Special Publication
NIST SP 800-63-4

Digital Identity Guidelines

David Temoshok
Ryan Galluzzo
Connie LaSalle
Naomi Lefkovitz *
Applied Cybersecurity Division
Information Technology Laboratory

Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Yee-Yin Choong
Information Access Division
Information Technology Laboratory

Diana Proud-Madruga
Sarbari Gupta
Electrosoft

* *Former NIST employee; all work for this publication was done while at NIST.*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-4

July 2025

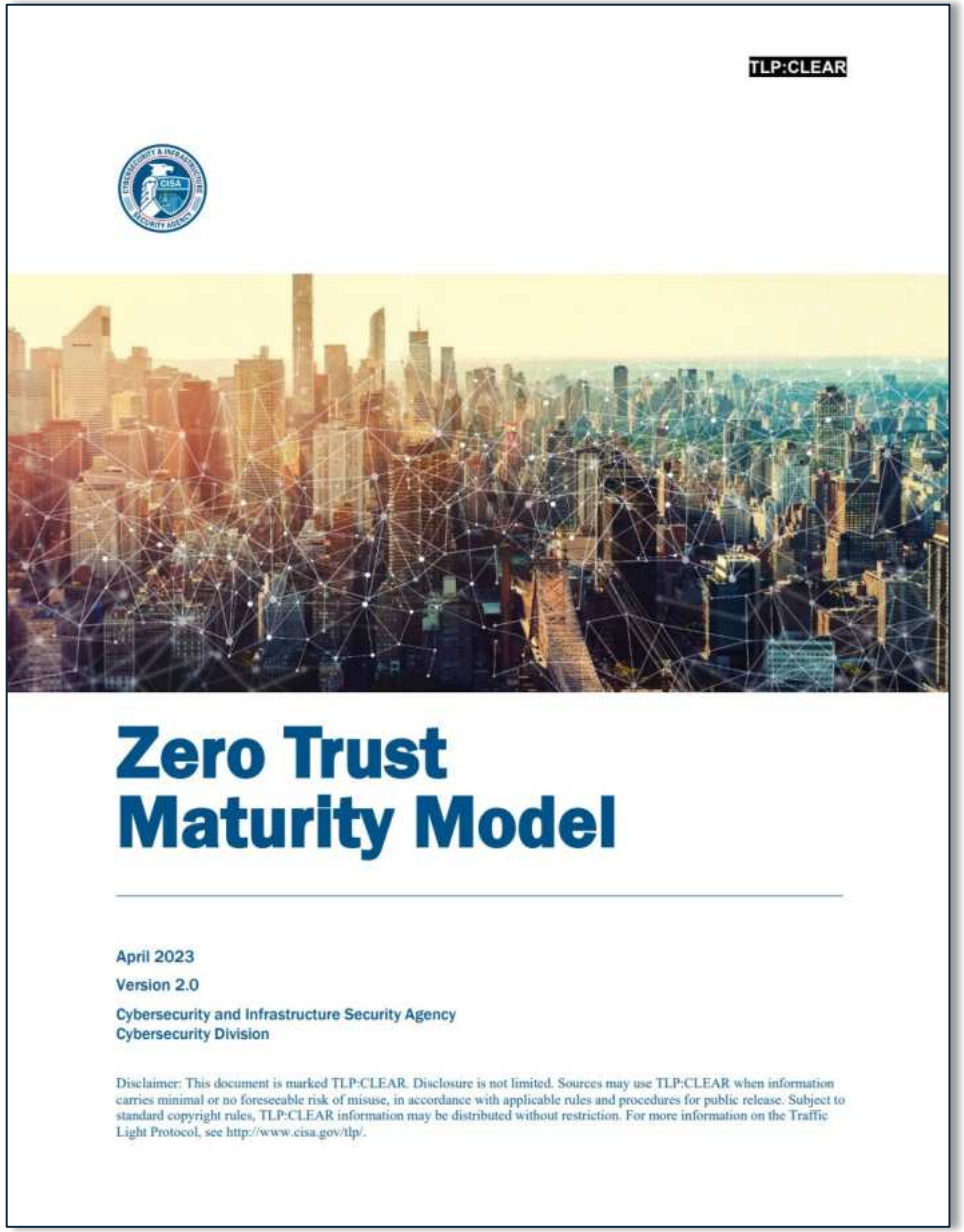
U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary for Standards and Technology and Acting NIST Director

Electrosoft

CISA Maturity Model

- **Traditional**
  - Authentication with static MFA, using passwords or tokens only at login without ongoing validation
- **Initial**
  - Authentication with MFA, combining passwords and contextual attributes (e.g., location or activity)
- **Advanced**
  - Authentication with phishing-resistant MFA, attributes, and implementation of password-less options such as FIDO2 or PIV
- **Optimal**
  - Continuous validation with phishing-resistant MFA throughout session



Electrosoft

From Static MFA to Continuous Authentication

Electrosoft

Taking Authentication to the Next Level

- **Workflow Changes**
  - Continuous Verification
  - Context Input (Risk Signals)
  - Real-Time Analysis
  - Dynamic Response
- **Risk Signals**
  - Device Health
  - Geolocation
  - IP Reputation
  - User Behavior
  - Application Sensitivity

- **Dynamic Response**
  - If anomalies detected, additional authentication factors (e.g., biometric check, token) required

Electrosoft

Sensitive Scenarios in Federal Environments

- **Non-Government Devices**
  - Login attempts from personal or non-GFE devices
- **Unusual Locations**
  - Access attempts from foreign locations
- **Suspicious Networks**
  - Connections from high-risk or anonymized sources
- **Sensitive Systems**
  - Access to HR, admin consoles, or financially relevant systems
- **Behavior anomalies**
  - Excessive failed logins or attempts to escalate privilege

Electrosoft

Best Practices and Implementation Approaches

Electrosoft

Translating Policy Into Action

- **Map policy requirements to mission needs**
  - Use OMB, NIST, CISA policy to ensure ZT compliance
- **Prioritize phishing-resistant MFA**
  - Implement PIV, FIDO2 to increase Authentication Assurance
- **Implement adaptive authentication**
  - Dynamically adjust authentication requirements based on risk context (e.g., device, location, behavior)
- **Integrate continuous monitoring, identity analytics, and artificial intelligence (AI)**
  - Establish baseline for detection of anomalies and response in real-time

Electrosoft

Practical Steps for Agencies

- **Prioritize high-risk systems**
  - Modernize complex and financially relevant systems first
- **Implement Attribute-Based Access Control (ABAC)**
  - Attribute-driven policies allow for more granularity and dynamic access
- **Invest in federation and interoperability**
  - Enable secure collaboration across agencies and external partners
- **Embrace emerging technologies and secure CI/CD pipeline**
  - Leverage AI, FedRAMP-approved, multi-cloud vendors and DevSecOps approach

Electrosoft

Wrap-Up

Electrosoft

Agency Factors for Success

- **Collaboration**
  - Leadership must set the tone
  - Cross-team collaboration is critical (e.g., Working Groups, Tiger Teams)
- **Implementation Considerations**
  - There should be a balance between user experience and security/usability
  - Pilots reduce risk before full deployment
- **Continuous Improvement**
  - Zero Trust is a journey, and not a one-time fix or quick patch

Electrosoft

Conclusion

- **Key Points**
  - Static MFA is foundational, but not sufficient to protect Federal identities
  - Continuous, risk-based authentication is central to Zero Trust and ICAM modernization
- **Recommendations**
  - Phishing-resistant MFA (PIV, FIDO2) should be prioritized
  - Integrate context checks (device, location, behavior) to increase identity assurance
- **Final Thoughts**
  - Zero Trust is a long-term commitment
  - Authentication strategies will need to continuously evolve

Electrosoft

Discussion and Contact Information

- **Dr. Nnamdi Osia**
  - Email: nosia@electrosoft-inc.com
  - LinkedIn: https://www.linkedin.com/in/nnamdiosia/
- **Electrosoft**
  - Web: http://www.electrosoft-inc.com
  - LinkedIn: https://www.linkedin.com/company/electrosoft/

Electrosoft