



ERMProtect Capabilities Statement

GSA Multiple Award Schedule Holder

SINs **54151HACS** (Highly Adaptive Cybersecurity Services) | **611420** (IT Training)

Trusted Cybersecurity. Human-First Delivery.

ERMProtect is a cybersecurity, digital forensics, and risk-management consulting firm with 25+ years of experience helping organizations protect systems, data, people, and mission-critical operations. Founded in 1998, ERMProtect delivers the depth and rigor of a large consulting firm with the agility, access, and pricing of a boutique partner.

Core Competencies

Cybersecurity Assessments & IT Audits (SIN 54151HACS)

- Enterprise cybersecurity assessments aligned with NIST CSF, NIST SP 800-53, ISO 27001, CIS, CRI, and more.
- Regulatory and compliance audits supporting PCI, FISMA, HIPAA, GLBA, FERPA, GDPR, FedRAMP, SOC 2, and industry-specific mandates.
- Third-party and vendor risk assessments to evaluate security posture and control effectiveness.

Penetration Testing & Adversarial Simulation (SIN 54151HACS)

- Comprehensive penetration testing across external and internal networks, web and mobile applications, wireless and cloud environments, AI-powered systems, ICS/SCADA and IoT, physical security, and social engineering.
- Actionable reporting focused on remediation, risk prioritization, and executive decision-making.

Digital Forensics & Incident Response (SIN 54151HACS)

- Digital forensics and incident response for data breaches, ransomware, fraud, insider misconduct, and litigation support.
- PCI forensic investigations and card-brand-mandated breach response.
- Cryptocurrency investigations, including transaction tracing and evidentiary support.

AI Strategy & Risk Management (SIN 54151HACS)

- Secure and responsible AI adoption advisory led by PhD-level AI experts
- AI strategy and governance supporting secure, responsible, mission-aligned adoption
- AI risk assessments and security testing
- Third-party AI vendor reviews to evaluate controls and risk

Co-Sourced Cybersecurity Services (SIN 54151HACS)

- Flexible delivery models including Virtual CISO, incident response, remediation, policy development, advisory services, and third-party vendor risk assessments

IT & Security Training (SIN 611420)

- Security awareness and technical training programs for federal, state, and commercial audiences
- LMS-based delivery, SCORM-compliant modules, and fully customized courses
- Training for both technical and non-technical audiences, including executives



Differentiators

- **25+ years** of proven cybersecurity experience
- **One of ~20 PCI PFI-certified firms worldwide**, authorized by major card brands to investigate payment-card breaches
- **Certified cybersecurity professionals** (CISSP, CEH, PCI QSA, PCI PFI, etc.)
- **Experience serving 450+ clients across 40+ industries**, including government and Fortune 500 organizations
- **Human-first delivery model** with direct access to senior experts and boutique pricing
- **Rapid deployment and scalable solutions** aligned to mission needs
- **Global reach** with multilingual training capabilities

Government Capabilities

ERMProtect provides trusted cybersecurity, compliance, and risk-management services to federal, state, and local government agencies. Our government engagements are delivered by senior-level consultants experienced in operating within regulated, high-security environments requiring discretion, confidentiality, and executive-level communication.

Government capabilities include:

- **Cybersecurity and information assurance** supporting complex government environments
- **Development and implementation** of cybersecurity policies, procedures, and governance frameworks
- **Enterprise risk assessments** aligned with NIST, FISMA, CJIS, and federal risk-management frameworks
- **Network security** architecture review, segmentation, and resilience planning
- **Incident response** planning, **breach investigation** support, and continuity planning
- **Penetration testing**, vulnerability assessments, and remediation advisory services
- **Security awareness, phishing simulations**, and executive-level cybersecurity training

Federal Past Performance

ERMProtect has supported U.S. federal civilian and defense agencies with cybersecurity, risk management, digital forensics, and compliance services across complex, distributed environments.

Department of Defense

- **Department of the Navy (NAVAIR)**: Developed a fully customized cybersecurity awareness program to promote secure employee practices.
- **Department of the Army**: Provided vulnerability management and database security solutions to identify misconfigurations, rogue installations, and network risks.
- **Defense Information Systems Agency (DISA)**: Supported multi-year PCI compliance and information security audit activities for the Defense Commissary Agency (DeCA) across a global infrastructure.
- **Defense Commissary Agency (DeCA)**: Performed highly technical PCI compliance and information-security audit services over a worldwide footprint.
- **Washington Headquarters Services (WHS)**: Supported threat detection and response capabilities through enterprise security technology implementation.



Department of Homeland Security

- **Federal Law Enforcement Training Center (FLETC):** Conducted security authorization and risk assessments in accordance with **FISMA, NIST SP 800-53A, OMB guidance, and DHS policy**, including enterprise-wide network authorization testing.
- **U.S. Citizenship and Immigration Services (USCIS):** Supported development and execution of a strategic cybersecurity awareness program delivering measurable risk-reduction outcomes.

Department of the Treasury

- **Bureau of the Public Debt:** Provided vulnerability management and database security solutions supporting enterprise risk reduction.
- **Office of the Comptroller of the Currency (OCC):** Supported asset discovery, network security, application security, and compliance monitoring capabilities.

Department of State

- **U.S. Agency for International Development (USAID):** Supported the design, installation, and configuration of network access control technology to protect agency data and enable secure enterprise access.

United States Postal Service (USPS)

- Provided **PCI/PFI digital forensic investigation services** in support of credit-card security incidents and breach response activities.

Company Data

- **UEI:** H52KHKAFHEH8 | **CAGE Code:** 5FDC2
- **Business Type:**
 - Minority-Owned Business
 - Women-Owned Small Business
 - Women-Owned Business
 - DOT Certified Disadvantaged Business Enterprise
 - Hispanic American Owned Business
 - SBA-Certified Women-Owned Small Business
- **GSA Contract Number:** 47QTCA26D0040
- **Period of Performance:** March 18, 2026 – March 17, 2031
- **Website:** ermprotect.com

Point of Contact

- Silka Gonzalez, President
- 305-335-7610, sgonzalez@ermprotect.com