LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

MARCH 2024

PROFESSIONAL DEVELOPMENT OF THE SECURITY WORKFORCE

When it comes to professional development, the LIS Solutions Security Team is dedicated to improving themselves by applying what they learn in government security trainings to their careers and to the security program.

LIS Security Professionals have access to a variety of security trainings, resources, job aids, seminars, networking, and tool kits that are always available to help them with their professional development.

Here is a list of a few trainings options that are available:

- Reporting Requirements
- Information Systems / Cyber Security
- Insider Threat / Active Shooter
- Supply Chain Risk Management
- OPSEC
- Counterintelligence
- General Security
- Physical Security

With these trainings, LIS Security Professionals will provide quality customer service to customers, candidates, and employees, by providing information to prevent, safeguard, and protect all assets. Although this information benefits your security professionals, it is also beneficial—and required by the government—for LIS employees to have access the information provided in these trainings.

Security education and training is helpful to better understand what adversaries want access to, and how you can protect yourself from threats or risks. It is our duty as your security professional to also have this same information available to you to not only empower you to protect yourself, but also to protect LIS Solutions.

This resource list will help you find the best places to access these security trainings and education:

- A simple Google search of the security topic you want to know.
- Center fore Development of Security Excellence (CDSE)
- Defense Counterintelligence and Security Agency DCSA

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

You have a responsibility to protect your information, but also LIS Solutions' information against threats and adversaries. It is our duty to know and recognize risks, threats, and vulnerabilities and apply what we have learned to mitigate the threats that exist today.

It is essential to be able to recognize:

1. Cyber intrusions and know how to protect your digital assets.
2. Know how to protect your physical assets and recognize the vulnerabilities.
3. Identifying and safeguarding your Personal Identifiable Information (PII).
4. The ability to know indicators of an insider threat or active shooter.

> **"When the number of security professionals available to get the job done, is only adequate, the expertise of those professionals must be excellent. CDSE security education, training, and certifications make that possible."**
>
> — Mark Haskett, CFM, SFPC
> Deputy Assistant Director for Securityand Facilities Naval Criminal Investigative Service

---

Read this article below at your leisure:

Borromeo, M. (2024, January 11). How Small Businesses Can Help Efficiently Mitigate Information Security Risks. **https://martechseries.com/mts-insights/guest-authors/how-small-businesses-can-help-efficiently-mitigate-information-security-risks/**