(U) OPSEC Course Descriptions:

*** (U) IOSS Computer-based Training (CBT) self-paced online training**

- **OPSE-1301: OPSEC Fundamentals.** This CBT provides a basic working knowledge of OPSEC with a focus on its use in the workplace. Upon completing this course, learners will be able to demonstrate their understanding of the OPSEC process, describe how they can contribute to a good OPSEC posture for their organization and assist leaders with OPSEC issues in a crisis situation.
- **Cyber OPSEC Awareness (2017).** This CBT focuses on understanding Cyber Threats and how to incorporate OPSEC practices to protect Cyber-related infrastructure and activities.
- **Critical Infrastructure OPSEC.** "What's in it for me" (2016). This training focuses on OPSEC as it relates to the following four Critical Infrastructure and Key Resources (CIKR) sectors: Financial Sector, Emergency Services Sector, Energy Sector, and Transportation Sector.
- **Additional CBTs** are available on the IOSS website.

*** (U) IOSS Instructor-led Online Courses**

- **OPSE-1500: OPSEC and Public Release Decisions.** This course addresses the OPSEC issues that should be considered when reviewing information for public release and public access. This course is specifically designed for individuals involved in determining what information should be released to the public, such as public affairs officers, web masters, Freedom of Information Act review staff, speech writers, speakers, classification review personnel, and OPSEC coordinators**.**
- **OPSE-2380: OPSEC Analysis.** This course will provide learners with extensive training on how to conduct OPSEC analysis. Learners will be able to develop lists of critical information and the value of each item, identify threats and their values, identify common vulnerabilities and their values, calculate estimated risk, and determine viable countermeasures for reducing risk, and brief senior leadership on their findings.
- **OPSE-2390:** Program Management. This course will provide learners with the knowledge needed to develop and sustain an effective OPSEC program. Upon completion of the course, learners will be able to identify the required components of an OPSEC program, outline the responsibilities of program managers and coordinators, develop organizational OPSEC policies, plan internal and external assessments, and develop a basic program budget.
- **OPSE-3500:** OPSEC and The Internet. This course introduces OPSEC practitioners to common threats, vulnerabilities, and countermeasures associated with the Internet. It will allow OPSEC practitioners to better assess the risk when using the Internet-based technologies.

(U) NOTE: The combined content of OPSE-2380 and OPSE-2390 is considered Level II OPSEC Training by most federal D/As and military organizations. Level II OPSEC Training is generally considered a requirement for OPSEC Program Managers.