## ManTech Advanced Systems International
### 2017 Security Training Schedule

### Risk Management Framework Course

<table>
<thead>
<tr>
<th>Course Dates</th>
<th>Course Location</th>
<th>Course Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 16 – 19, 2017</td>
<td>Joint Base Anacostia-Bolling, Washington, DC</td>
<td>$1,950.00</td>
</tr>
<tr>
<td>November 13 - 16, 2017</td>
<td>Emerald Coast Conference Center 1250 Miracle Strip Pkwy, SE Fort Walton Beach, FL 32548</td>
<td>$1,950.00</td>
</tr>
<tr>
<td>December 4 – 7, 2017</td>
<td>One Space Park, Bldg S, Conference Room 1275B, Redondo Beach, CA</td>
<td>$1,950.00</td>
</tr>
</tbody>
</table>

### Information Systems Continuous Monitoring

<table>
<thead>
<tr>
<th>Course Dates</th>
<th>Course Location</th>
<th>Course Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 10 – 12, 2017</td>
<td>Desert Willow Conference Center 4340 E Cotton Center Blvd. Phoenix, AZ 85040</td>
<td>$2,990.00</td>
</tr>
<tr>
<td>December 12 – 14, 2017</td>
<td>Desert Willow Conference Center 4340 E Cotton Center Blvd. Phoenix, AZ 85040</td>
<td>$2,990.00</td>
</tr>
</tbody>
</table>

### Program Security Fundamentals

<table>
<thead>
<tr>
<th>Course Dates</th>
<th>Course Location</th>
<th>Course Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 23 – 26, 2017</td>
<td>Joint Base Anacostia-Bolling, Washington, DC</td>
<td>$1,950.00</td>
</tr>
</tbody>
</table>

*NOTE: Dates, locations, prices and availability are subject to change. ManTech reserves the right to set a minimum number of registrations for each course conducted. No terms and conditions of any ordering document are binding on ManTech, and are null and void. ManTech shall only be bound to those terms and conditions executed by a duly authorized representative of ManTech.


**Maintaining Your 8570 Certification Requirements:**

**Risk Management Framework & Information Security Continuous Monitoring**
- CompTia CEU’s: 32 hours towards A+, Network+, and Security+
- ISC (2): CPU’s: 32 hours towards CAP, CISSP, and SSCP

**Maintaining Your SPeD Certifications**

**Program Security Fundamentals (PSF)**
- You may claim 45 PDU’s under category 2A when you attend this course. The hours will be reflected on your attendance certificate.
Coming Soon!!

Space Domain Awareness

With space becoming more contested, and congested, as well as increasingly integral to both the U.S. defense and economy, the U.S. Government (DOD and IC) is expected to receive a significant budget increase over the next FYDP to increase the resiliency of our space architecture. This course presents a detailed overview of the variety of threats that our systems face today, as well current tools, tactics and procedures that are available to combat these threats.

Onsite Courses

ManTech’s onsite training brings first-class training to your location so you may efficiently train your team all at the same time and location. You provide the facility and students and we’ll provide a top-level instructor and courseware. All ManTech courses apply practical knowledge and hands-on skills that can be applied immediately upon returning to the workplace.

**There are several benefits for training your team with an onsite course:**
- All students receive the same instruction and examples
- Practice the same labs and exercises
- Have an opportunity to discuss issues and concerns that relate to your organization
- Significant cost savings (students don’t have to travel, we come to you)

<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
<th>Cost</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management Framework</td>
<td>4 Days</td>
<td>$27,500.00</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*At customer provided facility</td>
<td></td>
</tr>
<tr>
<td>Information Systems Continuous</td>
<td>3 Days</td>
<td>$35,000.00</td>
<td>16</td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
<td>*At customer provided facility</td>
<td></td>
</tr>
<tr>
<td>Windows 7 Security Audit</td>
<td>2.5 Days</td>
<td>$37,500.00</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* At customer provided facility</td>
<td></td>
</tr>
<tr>
<td>Introduction to Linux Security</td>
<td>2.5 Days</td>
<td>$37,500.00</td>
<td>16</td>
</tr>
<tr>
<td>Fundamentals</td>
<td></td>
<td>* At customer provided facility</td>
<td></td>
</tr>
<tr>
<td>Program Security Fundamentals</td>
<td>4 Days</td>
<td>$27,500.00</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>4 Days</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>* At customer provided facility</td>
<td></td>
</tr>
</tbody>
</table>

If you are interested in purchasing an onsite course, contact Tamara Delesky at (703) 610-9297 or (540) 604-8245 / Tamara.Delesky@ManTech.com
ManTech Advanced Systems International
Risk Management Framework

1. The history and transformation of Risk Management Framework
   a. By the end of this module you should be able to:
      i. Understand Transformation Strategic Vision and Goals
      ii. Explain how the C&A process is transitioning to align with the RMF process
      iii. Explain the RMF Roles and Functions
      iv. Discuss Committee for National Security Systems (CNSS) policies and instructions; National Institute of Standard and Technology (NIST) Special Publications; and Joint SAP Implementation Guide (JSIG)
      v. Explain the Security Authorization Artifacts required to achieve system authorization

2. Managing Risk Within the SAP Information Environment
   a. By the end of this module you should be able to:
      i. Understand the basic concepts of Risk Management
      ii. Understand how to manage risk within the SAP information Environment
      iii. Define risk management factors, to include the risk analysis questions to be considered
      iv. Implement the Risk Management Framework and process in support of:
         1. NIST SP 800-37
         2. NIST SP 800-39
         3. NIST SP 800-30
      v. Understand the importance of Risk Management within the System Development Lifecycle

3. Step 1 – Categorizing the System
   a. By the end of this module you should be able to:
      i. Discuss Risk Management Framework Step 1 – System Categorization
      ii. Understand the initial Risk Assessment
      iii. Understand essential elements of Information and expectations for a System Security Plan (SSP)

4. Step 2 – Selecting Security Controls
   a. By the end of this module you should be able to:
      i. Explain the Risk Management Framework Step 2 – Selecting Security Controls
      ii. Gain awareness of the SAP Communities combined use of CNSS & NIST guidelines for NSS as process for Control Selection
      iii. Complete a Security Control Selection Exercise
      iv. Review and understand a Security Control Traceability Matrix (SCTM)
5. **Step 3 – Implementing Security Controls**
   a. By the end of this module you should be able to:
      i. Explain the Risk Management Framework Step 3 – Implementation of Security controls
      ii. Gain Awareness of the Special Access Program (SAP) community’s combines use of NIST guidelines for NSS and Community Best Practices for Implementing Security Controls
      iii. Discuss Best Practices to assist in implementing security controls

6. **Step 4 – Assessing Security Controls**
   a. By the end of this module you should be able to:
      i. Explain the Risk Management Framework Step 4 – Assessment of Security Controls
      ii. Gain awareness of the Special Access Program (SAP) community’s combined use of NIST guidelines for NSS and Community Best Practices for Assessing Security Controls
      iii. Discuss NIST SP 800-53A and Assessment Cases
      iv. Review Security Assessment Report Essential Elements of Information
      v. Discuss methods to assist in assessing Security Controls

7. **Step 5 – Security Authorization**
   a. By the end of this module you should be able to:
      i. Explain the Risk Management Framework Step 5 – System Authorization
      ii. Understand Plan of Action and Milestones (POA&M) Artifact
      iii. Understand types of system authorization

8. **Step 6 – Information Security Continuous Monitoring**
   a. By the end of this module you should be able to:
      i. Apply Risk Management Framework Step 6 – Continuous Monitoring
      ii. Describe SAP Information Security Continuous Monitoring Requirements and Implementation
      iii. Gain awareness of Configuration Management
      iv. Describe a Security Impact Analysis (SIA); Ongoing Controls Assessment; Reporting

9. **Best Practices and Tools**
   a. By the end of this module you should be able to:
      i. Share and discuss IA Best Practices
      ii. Understand various government and industry sites that can provide IA guidance and support
      iii. Various tools to assist the ISSM / ISSO
      iv. Discuss the use of various automated tools

Students will receive: Book with course slides, hard copy of latest JSIG, JSIG templates book, the DAAPM, PM RMF Handbook, and a reference CD
ManTech Advanced Systems International
Information Systems Continuous Monitoring (ISCM)

1. Cybersecurity Vulnerabilities & Threats to Information & Information Systems
   a. By the end of this module you should be able to:
      i. Discuss common vulnerabilities, threats and trends
      ii. Understand and discuss system exploits
      iii. Understand basic concepts of Risk
      iv. Understand Continuous Monitoring and Risk Management
      v. Discuss the Insider Threat
      vi. Define risk management factors, to include the risk analysis questions to be considered
      vii. Implement the Risk Management Framework and process in support of JSIG

2. Introduction to Information Security Continuous Monitoring
   a. By the end of this module you should be able to:
      i. Describe SAP Information Security Continuous Monitoring requirements and implementation
      ii. Be familiar with key documents and terms
      iii. Understand the roles and responsibilities
      iv. Understand why Continuous Monitoring and the way forward

3. Testing & Assessing Controls
   a. By the end of this module you should be able to:
      i. Discuss various technical controls
      ii. Understand the techniques for assessing controls
      iii. Understand the importance of proper control implementation to support assessment and continuous monitoring steps
      iv. Test and document the security configuration
      v. Discuss security assessment plan

4. Monitoring Controls Within the Security Automation Domains
   a. By the end of this module you should be able to:
      i. Discuss the eleven security automation domains that support continuous monitoring and the controls they monitor
      ii. Discuss what and how we monitor various security controls
      iii. Discuss the development of a continuous monitoring strategy
      iv. Discuss and use tools to monitor the various controls within the security automation domains
5. **ISCM Documentation Creation**  
a. By the end of this module you should be able to:  
   i. Discuss and provide sample plans  
   ii. Discuss the frequency selection  
   iii. Be familiar with various document creation and assistance tools  

6. **ISCM Best Practices & Reference Sources**  
a. By the end of this module you should be able to:  
   i. Share and discuss IA Best Practices  
   ii. Understand various government and industry sites that can provide IA guidance and support  
   iii. Various tools to assist the ISSM / ISSO  
   iv. Discuss the use of various automated tools
ManTech Advanced Systems International / LOGOS Secure
Windows 7 Security Audit (Onsite Course Only)

1. Audit Method and Policy
   a. By the end of this module you should be able to:
      i. Understand Audit Method and Policy
      ii. Discuss CNSS, NIST, NISPOM, PCI, HIPAA, FISMA
      iii. Understand when and how to use different methods for auditing
      iv. Discuss Best Practices for implementing audit method and policy

2. What’s New and Security Features
   a. By the end of this module you should be able to:
      i. Understand Windows 7 / Server 2008R2 New and Improved Audit Security Features
      ii. Discuss the applicable security features to be implemented
      iii. Summarize the intent of required security features
      iv. Explain the importance of proper configuration in order to conduct auditing relative to Policy Confirmation and/or Violation

3. Even Logs and EVTX
   a. By the end of this module you should be able to:
      i. Understand how to examine the new structure of even logs
      ii. Explain how to Note the addition of log types
      iii. Understand how to research the underlying technology of the new format and implications
      iv. Explain how to use the updated Event Viewer for viewing the new format and take advantage of queries

4. Audit Infrastructure
   a. By the end of this module you should be able to:
      i. Understand Audit Infrastructure
      ii. Identify preliminary concerns to accomplish collection with integrity
      iii. Understand how to analyze event logs
      iv. Discuss how to assess “your” situation and make determinations of “your” environments

5. Native Commands and Power Shell
   a. By the end of this module you should be able to:
      i. Review and understand Native Windows commands
      ii. Understand how to use important tools for Event Log Management
      iii. Gain awareness of how to use Power Shell
6. **Event Categories**  
a. By the end of this module you should be able to:  
   i. Understand the Windows Audit Policy  
   ii. Describe the various Event Types  
   iii. Identify the different Event Codes  
   iv. Review the Event Log and attempt to find out what it is telling us  
   v. Approach the information with RAM in mind to help us prepare for Queries  

7. **Tools / Log Parser**  
a. By the end of this module you should be able to:  
   i. Gain awareness of LogParser as a utility for audit reduction  
   ii. Understand how to create tools to make LogParser easier to use  
   iii. Discuss Windows 7 capabilities  

8. **VS Audit Framework**  
a. By the end of this module you should be able to:  
   i. Understand VS Audit Framework  
   ii. Explain how VS simplifies the challenges of using a Query Tool for less technical  
   iii. Explain VS Rapid Query Development  
   iv. Understand how to organize and practice our radical audit method  
   v. Discuss how VS provides for more advanced solutions  

9. **Query Eye for the Security Guy**  
a. By the end of this module you should be able to:  
   i. Explain how to analyze the reference data and apply the tools, methods and new knowledge  
   ii. Discuss current issues and Best Practices within the community
Introduction to Linux Security (Onsite Course Only)

The Introduction to Linux Security course is an intensive 2.5-day training experience led by seasoned Information System Security and Technology professionals. This course provides practice in advanced Information Systems Security skills to support the protection of information and information systems within an ICD 503/JSIG/RMF for DoD IT environment. During the course of instruction, the student will be able to apply Linux security features in order to adhere to requirements for Confidentiality, Integrity, and Availability. Each student will have the opportunity, through practical exercises and hands-on labs, to configure a Linux workstation to comply with ICD 503/JSIG/RMF for DoD IT technical security requirements.

The hands-on Introduction to Linux Security course addresses the array of government requirements faced by today’s ISSO/ISSM and System Administrators. The student leaves the class armed with the knowledge and tools required to ensure that their information system operates at an acceptable level of risk.

Course Content

The hands-on Introduction to Linux Security course addresses the array of government requirements faced by today’s IAO and System Administrators. The student leaves the class armed with the knowledge and tools required to ensure that their information system operates at an acceptable level of risk.

Topics discussed include:

- Risk Management Framework Overview
- Operating System and Root Account Security
- Linux Identification and Authentication Methods and Common Threats
- Use of Pluggable Authentication Modules
- Linux Resource and Session Control issues
- Methodology for Object Access and Discretionary Access Control
- Configuring and Conducting Auditing within a Linux Environment
ManTech Advanced Systems International
Program Security Fundamentals

1. Information Security
   a. By the end of this module you should be able to:
      i. Understand original and derivative classification for collateral and SAP information
      ii. Understand classification levels and categories
      iii. Apply appropriate classification markings
      iv. Maintain a Top Secret Accountability System
      v. Understand the function of the Document Control Center (DCC)
      vi. Properly handle security incidents and infractions

2. Operational Security (OPSEC)
   a. By the end of this module you should be able to:
      i. Identify the five parts of the OPSEC process, describe the specific activities involved in each part and explain ways to successfully accomplish these activities
      ii. Describe a number of associated OPSEC activities and explain how they relate to and facilitate accomplishment of the OPSEC mission
      iii. Apply what’s been learned to a practical exercise

3. Personnel Security (PERSEC)
   a. By the end of this module you should be able to:
      i. Understand different types of security questionnaires
      ii. Understand the different levels of security clearances
      iii. Become familiar with the agencies involved in the PERSEC process
      iv. Review form submission for completeness and accuracy
      v. Understand Program Access Requests (PAR’s)
      vi. Describe reporting requirements

4. Physical Security
   a. By the end of this module you should be able to:
      i. Comprehend, interpret, and identify Special Access Program Facility (SAPF) and Sensitive Compartmented Information Facility (SCIF) basic construction requirements
      ii. Create and process associated accreditation documentation for a new SCIF/SAPF
      iii. Discuss and consult with other physical security professionals about related topics, interface with technical teams, and process related documentation for Program Security Officer approvals
5. **Industrial Security**
   a. By the end of this module you should be able to:
      i. Identify, interpret, and explain Industrial security elements as they pertain to the government and industry partnership for operating in a Special Access Program (SAP) environment
      ii. Determine contractual security requirements and author a Contract Security Classification Specification, DD Form 254

6. **Information Systems Security**
   a. By the end of this module you should be able to:
      i. Comprehend, review and evaluate documentation necessary to assist in the operations of Information Systems and Information Assurance within a Special Access Program Facility (SAPF) and Sensitive Compartmented Information Facility (SCIF)
      ii. Gain working knowledge that will enable the collaboration with Information Assurance Managers (IAM) and Information Assurance Officers (IAO) to ensure Information Systems meet operational requirements

7. **Other Program Security Topics, Duties and Responsibilities**
   a. By the end of this module you should be able to:
      i. Create and implement a comprehensive security education and training program
      ii. Appreciate a very contemporary topic – Insider Threat!
      iii. Apply basic planning principles to a variety of program security planning requirements
      iv. Acquire a basic understanding of the Freedom of Information Act and how it impacts special access programs
      v. Apply various special security processes to the acquisition security arena
      vi. Manage inspection programs and perform special access security self-inspections