National Cyber Range Complex

Sample NCRC Range Event Schedule

Version 1.0

January 21, 2020

DISTRIBUTION STATEMENT F

DISTRIBUTION ONLY AS DIRECTED BY THE DIRECTOR, NATIONAL CYBER RANGE COMPLEX (NCRC). REQUESTS FOR THIS DOCUMENT MUST BE SUBMITTED TO THE OFFICE OF THE DIRECTOR, NATIONAL CYBER RANGE COMPLEX (NCRC).

EXPORT CONTROLLED

THIS DOCUMENT CONTAINS TECHNICAL DATA WHOSE EXPORT IS RESTRICTED BY THE ARMS EXPORT CONTROL ACT (TITLE 22, U.S.C., SEC 2751, ET SEQ.) OR THE EXPORT ADMINISTRATION ACT OF 1979 (TITLE 50, U.S.C., APP 2401 ET SEQ.) AS AMENDED. VIOLATIONS OF THESE EXPORT LAWS ARE SUBJECT TO SEVERE CRIMINAL PENALTIES. DISSEMINATE IN ACCORDANCE WITH PROVISIONS OF DOD DIRECTIVE 5230.25

1. Introduction

The intent of this document is to provide potential EPOS Offerors with an overview of a representative sample notional NCRC event schedule that can be used as a backdrop for estimating the numbers of personnel, types of skills, job families and levels of effort (LOE) required to successfully execute events on the NCRC.

The document presents a notional but representative sample schedule of one (1) year of events covering the expected base year of EPOS execution. The events used to develop this sample notional schedule are representative of past NCRC events in terms of number or events, types of events and concurrency of events.

1.1 Document Organization

The document is divided into the following sections:

- Section 1 provides basic introductory material
- Section 2 presents the sample notional NCRC event schedule
- Section 3 provides a more detailed description of each event to include an overview of the event, a description of the composition of the event environment and additional detailed information about the specific software that will be used for the event.

Note – This schedule and the events are representative of past NCRC events; however, the events described in the schedule are fictitious. Given the fictitious nature of the events included in this sample schedule, the Government will not comment on or provide any additional information about the specific lists of components, capabilities, hardware and software provided herein.

1.2 Characterization of Test and Training Events

The following sections provide a generalized characterization of NCRC events. Each event includes planning, design/configuration, and execution ~~and~~ activities. The post-execution sets of activities~~.~~ do not significantly vary based on event size.

1.2.1 Small Cyber Security Test Event

- Planning: Localized evaluation of a somewhat simplistic software/application. Minimal timeframe (1 month) required to work with the User to understand requirements and requirements are straightforward. May be the first in a series of events with the first instance focused on a relatively simple aspect in order to establish a baseline.

- Design/Configuration: Minimal development. Minimal setup of the range infrastructure. Limited variation platform configurations.
- Execution: Straightforward plan for Cyber Security Evaluation Team (CSET) assessment. CSET assessment may be conducted within a week but could take two weeks. CSET focused on gaining an initial understanding of security posture.

1.2.2 Medium Cyber Security Test Event

- Planning: System may include several components and/or Hardware in the Loop (HWIL). Several planning sessions (1-2 months) required to understand the system under test. May be a follow-on event to a successive series where the assessment is graduating in complexity.
- Design/Configuration: Limited development. Limited coordination required with User SMEs to assist with integration and setup. Straightforward range infrastructure setup.
- Execution: CSET assessment conducted over a two-week timeframe. CSET may need to meet with system SMEs to better understand how to structure the test. If this is a follow-on to a prior event, the CSET may include focus on evaluating improvement of security posture from the prior test.

1.2.3 Large Cyber Security Test Event

- Planning: Complex system of systems and/or integration of Hardware-in-the-Loop (HWIL). A few months of planning sessions (2-3) required to understand the systems under test. Possibly requiring an offsite Technical Exchange Meeting (TEM) with Subject Matter Experts (SMEs) and mission operators. Complex system of systems and/or integration of HWIL. May be follow-on of prior events with increasing complexity to address system of systems perspective
- Design/Configuration: Complex setup of range infrastructure which could include reverse engineering required by range engineers to effectively accommodate virtual and physical aspects. Setup can include multiple variations of platform configurations and instrumentation requirements. Review of technical documentation. Coordination with SMEs required to support installation and configuration of complex mission software/components.
- Execution: CSET assessment conducted over a two to three-week timeframe. CSET plan is detailed and worked in conjunction with SMEs.

1.2.4 Small Cyber Security Training Event

- Planning: Simplistic environment buildout leveraging re-use from other baseline environments: red, gray, blue; simple traffic generation and web content. Minimal timeframe required to work with the User to understand environment details. May be focused on individual team certification and training.
- Design/Configuration: Straightforward environment setup, leveraging prior capabilities previously developed. No new development or limited development of capabilities.
- Execution: Straightforward event execution timeframe, on-line for a week or two. Limited engagement by engineering team required while the event is executing.

1.2.5 Medium Cyber Security Training Event

- Planning: Moderately complicated environment. Several detailed meetings with the User to identify requirements, understand Master Scenario Event Lists (MSELs), and the scenario. Discussion to understand customization needed to support training objectives and scenario development. May be focused on multiple team training and readiness.
- Design/Configuration: Robust red, blue and gray space with realistic internet services and customized traffic generation to enable a representative target environment. High fidelity, realistic, and dynamic content. Combination of re-use of existing capabilities and new development. Integration of User tools. Can include Hardware in the loop.
- Execution: Support for event environment reconnaissance activities established on the range, pre-event execution and support during event execution based on dynamic requirements that may evolve during the course of the exercise. Event execution can be between one to two weeks.

1.2.6 Large Cyber Security Training Event

- Planning: Highly fidelity, realistic, complex training environment. Detailed meetings and official planning conferences to coordinate requirements for the training audience. May involve collaboration with other range providers to identify integration / touch points. Most often focused on support to large COCOM training exercises. Can include multi-national partners.
- Design/Configuration: High-fidelity, operationally realistic environments that mimic real-world behavior and performance. Large environment with significant number of diverse enclaves. Representative military and critical infrastructure target sets, representative ISPs, simulated satellite links, integration of wireless assets, integration of multiple hardware in the loop devices/components. Significant development of new

and/or tailored capabilities. Integration of User VMs and tools. Development of threat scenarios. Multi-level workflows representative of real-world performance.

- Execution: Environment ready approximately a month in advance of event execution to support user account management, reconnaissance, and other preparations. Event Execution for about two weeks. On-site support at primary exercise location to assist Users. Assess opportunity to address ad-hoc, dynamic, on-demand requirements as they emerge. Support for a significant number of multiple participants remotely connected.

1.3 General Notes and Information

- The time allocated each activity in the event descriptions, e.g. range configuration, network familiarization, reconnaissance (RECCE), event execution and post-event activities includes the time necessary to produce the related event products. Post-Event analysis time is intended to cover the development and delivery of all associated post-event CDRLs.
- The SW listed with each event description is the "core" event environment SW that is deployed by the NCRC automated tool suite. It does not include the additional SW that would be required to provide event specific capabilities like website content, content management systems, video and audio streaming, collaboration, functional databases, interactive websites, etc.
- Assume that 85% of the software listed for each event will be installed using the NCRC Automated Tool Suite. The other 15% will have to be installed manually. Unless otherwise noted, the hardware and software that is listed with each event description can be assumed to be part of the NCRC inventory; therefore, proposals do not need to include costs for that HW/SW.

1.4 Extending the Schedule

The sample schedule currently contains one (1) year worth of events for the expected EPOS Base Year. For evaluation purposes, the sample schedule for Option Year 1 will be the same events as the Base Year with each event being run twice and spread across the entire 12 months.

2. Sample NCRC EPOS Base Year Notional Event Schedule

Legend	
Bold	**Range Prep**
Bold (Underline)	**Execution week**

Regular (Not Bold)	Post-Event Week
Italics	***Faraday Cage Required***

In the notional range schedule below, each event is numbered and indicated by a separate color. Weeks including federal holidays are indicated with a red fill.

~~This notional schedule is for FY21 with an assumption of contract award by the beginning of FY21.~~ No events are indicated on the schedule for the first 90 days ~~(October through December)~~. During this 90-day period, contractors will be ramping up, receiving NCRC EPOS initial training and meeting other personnel training and security requirements in the contract/task order in preparation to commence work. Events are shown on the schedule to start in ~~January~~Month 4 of the base year and run through ~~September~~Month 12.

.

Unclassified // For Official Use Only

EPOS Base Year (FY21) Range Schedule
(Notional For Planning Purposes Only)

Events		October			
		5-Oct	12-Oct	19-Oct	26-Oct
Testbeds	1				
	2				
	3				
	4				
	5				
	6				
	7				
	8				
	9				

Events		November				
		2-Nov	9-Nov	16-Nov	23-Nov	30-Nov
Testbeds	1					
	2					
	3					
	4					
	5					
	6					
	7					
	8					
	9					

Unclassified // For Official Use Only

Unclassified // For Official Use Only

EPOS Base Year Range Schedule
(Notional For Planning Purposes Only)

Testbeds / Events	Month 1			
	Week 1	Week 2	Week 3	Week 4
1				
2				
3				
4				
5				
6				
7				
8				
9				

Testbeds / Events	Month 2				
	Week 1	Week 2	Week 3	Week 4	Week 5
1					
2					
3					
4					
5					
6					
7					
8					
9					

Unclassified // For Official Use Only

Unclassified // For Official Use Only

EPOS Base Year (FY21) Range Schedule
(Notional For Planning Purposes Only)

Testbeds	December			
Events	7-Dec	14-Dec	21-Dec	28-Dec
1				Range Shutdown
2				
3				
4				
5				
6				
7				
8				
9				

Testbeds	January			
Events	4-Jan	11-Jan	18-Jan	25-Jan
1	Test 21-1	Test 21-1	Test 21-1	Test 21-1
2	Training 21-1	Training 21-1	Training 21-1	Training 21-1
3				Test 21-2.1
4				
5				
6				
7				
8				
9				

Unclassified // For Official Use Only

Unclassified // For Official Use Only

EPOS Base Year (FY21) Range Schedule
(Notional For Planning Purposes Only)

Testbeds	February			
Events	1-Feb	8-Feb	15-Feb	22-Feb
1	Test 21-1	Test 21-1	Test 21-3	Test 21-3
2	Training 21-1	Training 21-1	Training 21-1	Test 21-4
3	Test 21-2.1	Test 21 -2.1	*Test 21-2.1*	*Test 21-2.1*
4				
5				
6				
7				
8				
9				

Testbeds	March				
Events	1-Mar	8-Mar	15-Mar	22-Mar	29-Mar
1	*Test 21-3*	*Test 21-3*	Test 21-3	Test 21-5	Test 21-5
2	Test 21-4	Test 21-4	Test 21-4	Test 21-4	Test 21-4
3	Test 21-2.1	Training 21-2	Training 21-2	Training 21-2	Training 21-2
4					
5					
6					
7					
8					
9					

Unclassified // For Official Use Only

Unclassified // For Official Use Only

EPOS Base Year (FY21) Range Schedule
(Notional For Planning Purposes Only)

Testbeds	Events	April			
		5-Apr	12-Apr	19-Apr	26-Apr
	1	Test 21-5	Test 21-5	Test 21-5	Test 21-5
	2	Test 21-6	Test 21-6	Test 21-6	Test 21-6
	3	Training 21-2	Training 21-2	Training 21-2	Training 21-2
	4				
	5				
	6				
	7				
	8				
	9				

Testbeds	Events	May				
		3-May	10-May	17-May	24-May	31-May
	1	Test 21-7	Test 21-7	Test 21-7	*Test 21-7*	*Test 21-7*
	2	Test 21-6	Test 21-6	Training 21-3	Training 21-3	Training 21-3
	3	Training 21-2	Test 21-8	Test 21-8	Test 21-8	Test 21-8
	4					
	5					
	6					
	7					
	8					
	9					

Unclassified // For Official Use Only

Unclassified // For Official Use Only

EPOS Base Year (FY21) Range Schedule
(Notional For Planning Purposes Only)

Testbeds	Events	June			
		7-Jun	14-Jun	21-Jun	29-Jun
	1	Test 21-7	Test 21-11	Test 21-11	Test 21-11
	2	Training 21-3	Training 21-3	Training 21-3	Test 21-2.2
	3	Test 21-8	Test 21-8	Test 21-10	Test 21-10
	4	Test 21-9	Test 21-9	Test 21-9	Test 21-9
	5				
	6				
	7				
	8				
	9				

Testbeds	Events	July			
		5-Jul	12-Jul	19-Jul	26-Jul
	1	Test 21-11	Test 21-11	Test 21-11	Test 21-12
	2	Test 21-2.2	Test 21-2.2	Test 21-2.2	Test 21-2.2
	3	Test 21-10	Test 21-10	Test 21-10	Test 21-10
	4	Test 21-9	Test 21-9	Training 21-4	Training 21-4
	5				
	6				
	7				
	8				
	9				

Unclassified // For Official Use Only

Unclassified // For Official Use Only

EPOS Base Year (FY21) Range Schedule

Testbeds	August				
Events	2-Aug	9-Aug	16-Aug	23-Aug	30-Aug
1	Test 21-12	Test 21-12	Test 21-12	Test 21-12	Test 21-12
2	Test 21-2.2	Training 21-5	Training 21-5	Training 21-5	Training 21-5
3	Training 21-4	Training 21-4	Training 21-4	Test 21-2.3	Test 21-2.3
4	Test 21-13	Test 21-13	Test 21-13	Test 21-13	Test 21-13
5					
6					
7					
8					
9					

Testbeds	September			
Events	6-Sep	13-Sep	20-Sep	27-Sep
1	Test 21-2.3	Test 21-2.3	Test 21-2.3	Test 21-2.3
2	Training 21-5	Training21 -5	Training 21-5	Training 21-5
3	Test 21-13			
4				
5				
6				
7				
8				
9				

Unclassified // For Official Use Only

Unclassified // For Official Use Only

EPOS Base Year Range Schedule
(Notional For Planning Purposes Only)

Testbeds Events	Month 3			
	Week 1	Week 2	Week 3	Week 4
1				Range Maintenance Shutdown
2				
3				
4				
5				
6				
7				
8				
9				

Testbeds Events	Month 4			
	Week 1	Week 2	Week 3	Week 4
1	Test 21-1	Test 21-1	Test 21-1	Test 21-1
2	Training 21-1	Training 21-1	Training 21-1	Training 21-1
3				Test 21-2.1
4				
5				
6				
7				
8				
9				

Unclassified // For Official Use Only

Unclassified // For Official Use Only

EPOS Base Year Range Schedule
(Notional For Planning Purposes Only)

Events		Month 5			
		Week 1	Week 2	Week 3	Week 4
Testbeds	1	Test 21-1	Test 21-1	Test 21-3	Test 21-3
	2	Training 21-1	Training 21-1	Training 21-1	Test 21-4
	3	Test 21-2.1	Test 21 -2.1	*Test 21-2.1*	*Test 21-2.1*
	4				
	5				
	6				
	7				
	8				
	9				

Events		Month 6				
		Week 1	Week 2	Week 3	Week 4	Week 5
Testbeds	1	*Test 21-3*	*Test 21-3*	Test 21-3	Test 21-5	Test 21-5
	2	Test 21-4	Test 21-4	Test 21-4	Test 21-4	Test 21-4
	3	Test 21-2.1	Training 21-2	Training 21-2	Training 21-2	Training 21-2
	4					
	5					
	6					
	7					
	8					
	9					

Unclassified // For Official Use Only

Unclassified // For Official Use Only

EPOS Base Year Range Schedule
(Notional For Planning Purposes Only)

Testbeds	Events	Month 7			
		Week 1	Week 2	Week 3	Week 4
	1	Test 21-5	Test 21-5	Test 21-5	Test 21-5
	2	Test 21-6	Test 21-6	Test 21-6	Test 21-6
	3	Training 21-2	Training 21-2	Training 21-2	Training 21-2
	4				
	5				
	6				
	7				
	8				
	9				

Testbeds	Events	Month 8				
		Week 1	Week 2	Week 3	Week 4	Week 5
	1	Test 21-7	Test 21-7	Test 21-7	*Test 21-7*	*Test 21-7*
	2	Test 21-6	Test 21-6	Training 21-3	Training 21-3	Training 21-3
	3	Training 21-2	Test 21-8	Test 21-8	Test 21-8	Test 21-8
	4					
	5					
	6					
	7					
	8					
	9					

Unclassified // For Official Use Only

Unclassified // For Official Use Only

EPOS Base Year Range Schedule
(Notional For Planning Purposes Only)

Testbeds	Events	Month 9			
		Week 1	Week 2	Week 3	Week 4
	1	Test 21-7	Test 21-11	Test 21-11	Test 21-11
	2	Training 21-3	Training 21-3	Training 21-3	Test 21-2.2
	3	Test 21-8	Test 21-8	Test 21-10	Test 21-10
	4	Test 21-9	Test 21-9	Test 21-9	Test 21-9
	5				
	6				
	7				
	8				
	9				

Testbeds	Events	Month 10			
		Week 1	Week 2	Week 3	Week 4
	1	Test 21-11	Test 21-11	Test 21-11	Test 21-12
	2	Test 21-2.2	Test 21-2.2	Test 21-2.2	Test 21-2.2
	3	Test 21-10	Test 21-10	Test 21-10	Test 21-10
	4	Test 21-9	Test 21-9	Training 21-4	Training 21-4
	5				
	6				
	7				
	8				
	9				

Unclassified // For Official Use Only

Unclassified // For Official Use Only

EPOS Base Year Range Schedule

Testbeds	Events	Month 11				
		Week 1	Week 2	Week 3	Week 4	Week 5
	1	Test 21-12	Test 21-12	Test 21-12	Test 21-12	Test 21-12
	2	Test 21-2.2	Training 21-5	Training 21-5	Training 21-5	Training 21-5
	3	Training 21-4	Training 21-4	Training 21-4	Test 21-2.3	Test 21-2.3
	4	Test 21-13	Test 21-13	Test 21-13	Test 21-13	Test 21-13
	5					
	6					
	7					
	8					
	9					

Testbeds	Events	Month 12			
		Week 1	Week 2	Week 3	Week 4
	1	Test 21-2.3	Test 21-2.3	Test 21-2.3	Test 21-2.3
	2	Training 21-5	Training21 -5	Training 21-5	Training 21-5
	3	Test 21-13			
	4				
	5				
	6				
	7				
	8				
	9				

Unclassified // For Official Use Only

3. Sample Event Descriptions

Test Event 21-1		
Description: Test Event 21-1 is a medium sized test event that involves a cybersecurity assessment of a new version of an already fielded Service capability. The goal is to increase the user's understanding of impacts of new products on the cybersecurity posture and operational employment of the new capability version. The event will include a cooperative vulnerability assessment and traditional penetration testing activities. • The event environment will consist of a single enclave and VLAN with AD, DNS, SQL, Exchange and SharePoint instances along with the User provided SUT (system under test) SW The event environment will have 7 ESXi hypervisors and 19 VMs. This event will not require any traffic generation.		
External Connections: N/A	**Event Classification:** Secret	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Test Event 21-1 will include 4 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution and 1 week of post-event activities.		

Software Overview							
# of Nodes Containing or Running the SW	**# of Types of Nodes Running the SW**		**Software Application Name**		**# of Nodes Containing or Running the SW**	**# of Types of Nodes Running the SW**		**Software Application Name**
1	1		CentOS 5.3 x64					
19	17		Meinberg NTP Client					

18	16		SSL Certs					
11	11		Windows 2008 R2 SP1					
4	4		Windows 2012 R2 Server x64					
3	1		Windows 7 Enterprise SP1 x64					
1	1		Yum Repo					
36	32		wget for Windows					
1	1		SUT (User Provided SW)					

Training Event 21-1		
Description: Training Event 21-1 will be a "Capture the Flag" style of training event where Cyber Protection Teams (CPTs) are able to hone their skills and TTPs in both competitive and non-competitive conditions. This event will have a naval flavor for which the NCRC will provide an event environment replicating 3 different kinds of ships each with 3 different "flags" that teams must find in order to disable each ship. Each participating team will be given access to an identical environment for a set time period during which they must capture as many 'flags' as possible. • The event environment will consist of a simplified Internet enclave with minimal services including a single Root DNS server and NTP services. A set of Blue enclaves will be provided for each type of ship that sit behind a DMZ as well as a small DODIN enclave with common network infrastructure services. • Traffic generation (TG) will be provided via Mantra and include web and E-mail. The event environment will have 2 ESXi hypervisors, 250 VMs and 200 nodes set up for Traffic Generation using Mantra.		
External Connections: Joint Information Operations Range (JIOR) connections to multiple locations.	**Event Classification:** Secret	**Faraday Cage**: N/A
User Participation: User personnel will not be on site during event execution.	**CSET Participation:** N/A	
Event Timeline: Training Event 21-1 will include 2 months of planning, 4 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 2 weeks of post-event analysis.		

Software Overview							
# of Nodes Containing or Running the SW	**# of Types of Nodes Running the SW**		**Software Application Name**	**# of Nodes Containing or Running the SW**	**# of Types of Nodes Running the SW**		**Software Application Name**
180	22		Adobe Acrobat Reader 9.3	5	5		Microsoft DNS Server Surrogate Software

3	3		Apache 2.2.15 HTTP Server Linux		5	5		Microsoft Exchange Server 2010 SP2 Enterprise
4	4		Apt Repo		5	5		Microsoft Windows Internet Information Server 2000
1	1		Bind 9.8.1 for Linux		8	8		MySQL 5.1
32	32		CentOS (multiple versions)		1	1		NTP Server
4	4		DHCP Server		180	22		Office 2010
4	4		Firewall		13	13		PHP 5.4
					188	23		Pidgin
1	1		Elastic Search		28	14		SSH Server
188	23		Firefox 35.0.1		2	2		Samba
5	5		Domain Controller Surrogate Software		4	4		Ubuntu 12.04 x64
16	2		Kali 2017.1		18	18		VyOS 1.1.6 x64
1	1		Kibana		4	1		Windows 2008 Enterprise SP1 x64
1	1		Logstash		17	17		Windows 2008 R2 SP1
1	1		MS SQL Server 2012 Enterprise SP1 x64		180	22		Windows 7 Professional SP1 x64
237	72		Mantra		32	32		Yum Repo
62	55		Meinberg NTP Client		3	3		ejabberd XMPP Server
2	2		Microsoft .NET Framework 3.5 SP1		402	80		wget for Windows
1	1		Microsoft DHCP Server Surrogate Software					

Test Event 21-2.1		
Description: Test Event 21-2.1 is the first in a series of large-scale test events that will independently test and evaluate commercial Industrial Control System (ICS) technologies and products and how they might be applied and integrated in analogous DoD systems. The event will include a cooperative vulnerability assessment and traditional penetration testing activities. • The event environment will consist of a small Internet enclave and an internal enclave behind a DMZ with sub-enclaves for 2 control enclaves and a building enclave that acts as the SUT. The User will provide the commercial products that are to be tested and the vendors will provide technical assistance as needed for their products. The event environment will have no hypervisors and 54 nodes set up for Traffic Generation using Mantra.		
External Connections: N/A	**Event Classification:** Secret	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Test Event 21-2.1 will include 5 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 4 weeks of post-event analysis.		

Software Overview

# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name		# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name
50	3		Adobe Acrobat Reader 9.3		2	2		Microsoft DNS Server Surrogate
50	3		Adobe Flash Player 11.5		2	2		Microsoft Exchange Server 2010 SP2 Enterprise
1	1		Apache 2.2.15 HTTP Server Linux		50	3		Microsoft Office 2007 Professional SP2
2	2		Apt Repo		1	1		PHP Default for Linux

1	1		Firewall		15	15		SSH Server
2	2		Windows Fileshare		1	1		Syslog Client
1	1		Elastic Search		1	1		Syslog Server
2	2		Domain Controller Surrogate		2	2		Ubuntu 12.04 x64
7	7		Kali 2.0 x64		5	5		Vyatta 6.6 x64
7	7		Kali Linux Full		1	1		Windows 2000 Server SP4 x86
1	1		Kibana		1	1		Windows 2003 Enterprise SP2 x86
1	1		Logstash		8	8		Windows 2008 R2 SP1
1	1		MS SQL Server 2012 Enterprise SP1 x64		1	1		Windows 2012 R2 Server x64
72	25		Mantra		54	7		Windows 7 Enterprise SP1 x64
1	1		Meinberg NTP Client		2	2		Windows XP Professional SP2 x64
2	2		Microsoft DHCP Server Surrogate		130	36		wget for Windows

Test Event 21-3		
Description: Test Event 21-3 is a complex large-scale event with a primary goal of assessing the security posture of a specific portion of a small sized Unmanned Ground Vehicle (UGV) that provides land-based tactical reconnaissance, surveillance, and target acquisition (RSTA) data collection. The NCRC will be deploying a detailed representation of the C2 portion of the UGV's supporting real-world networking infrastructure using information and VMs supplied by the User. The OGV will be operated and stimulated from within the NCRC faraday cage. Both the UGV and associated C2 applications will be provided by the User. • The event environment will consist of the UGV, UGV C2 application enclave, RF communications and stimulation HW/SW, the UGV C2 application as well as supporting SW and instrumentation. This event will include traditional penetration testing activities using User supplied tools and data to be performed by NCRC personnel working with User SMEs. The event environment will have 2 ESXi hypervisors and 35 VMs with no Traffic Generation.		
External Connections: N/A	**Event Classification:** TS/SCI	**Faraday Cage**: Required
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Test Event 21-3 will include 6 weeks of planning, 2 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 4 weeks of post-event analysis.		

Software Overview

# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name		# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name
34	5		Adobe Acrobat Reader 9.3		1	1		Microsoft Windows Internet Information Server 2000
34	5		Adobe Flash Player 11.5		1	1		MySQL 5.1
1	1		Bind 9.8.1 for Linux		2	2		PHP 5.4
1	1		CentOS 6.5 x64		2	2		SSH Server

6	6		Firewall		34	5		SSL Certs
34	5		Firefox 35.0.1		3	3		VyOS 1.1.6 x64
4	4		Domain Controller Surrogate Software		11	11		Vyatta 6.6 x64
57	28		Mantra		8	8		Windows 2008 R2 SP1
62	33		Meinberg NTP Client		5	5		Windows 2012 R2 Server Update x64
1	1		Microsoft DHCP Server Surrogate Software		34	5		Windows 7 Professional SP1 x64
4	4		Microsoft DNS Server Surrogate Software		1	1		Yum Repo
2	2		Microsoft Exchange Server 2010 SP2 Enterprise		94	36		wget for Windows
34	5		Microsoft Office 2007 Professional Edition w/SP2 Bundled					

Test Event 21-4

Description: Test Event 21-4 is the latest medium sized event in a series of events that the NCRC has hosted for a Program Office responsible for developing autonomous vehicle wireless control systems for use in non-deployed garrison environments. This event will continue the work done during previous events to refine the baseline configurations of User provided GOTS security applications prior to them being deployed. Specifically, this event will focus on non-RF portions of the system and assess and conduct a performance and security capabilities analysis of one component of a larger system.

- The event environment will consist of a small Internet enclave and an internal enclave behind a DMZ with a sub-enclave to host the SUT.

The event environment will have 2 ESXi hypervisors and 25 nodes for Traffic Generation using Mantra.

External Connections: N/A	**Event Classification:** Secret	**Faraday Cage**: N/A

User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required

Event Timeline: Test Event 21-4 will include 3 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 2 weeks of post-event analysis.

Software Overview

# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name		# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name
1	1		Apache 2.2.15 HTTP Server Linux		1	1		Logstash
12	3		Apt Repo		35	26		Mantra
2	2		CentOS 7.0 x64		1	1		Meinberg NTP Client
1	1		Chrome 43.0.2357.65		1	1		PHP Default for Linux
4	4		Firewall		35	26		SSH Server

1	1		Elastic Search		12	11		Ubuntu 12.04 x64
10	1		FTP Server		9	9		VyOS 1.1.6 x64
3	3		Firefox 35.0.1		11	11		Windows 7 Professional SP1 x64
13	4		Gnome Desktop		1	1		Wireshark 2.0.3 for Windows
10	10		Kali 2.0 x64		2	2		Yum Repo
1	1		Kibana		22	22		wget for Windows

Test Event 21-5		
Description: Test Event 21-5 will be the latest in a series of events that the NCRC has hosted for a Program Office responsible for developing enterprise security solutions for use in deployed environments. This event will continue the work done during previous events to refine the baseline configurations of User provided commercial security applications prior to them being deployed. Specifically, this event will assess and conduct a performance and security capabilities analysis of one component of a larger system. • The event environment will consist of a simplified Internet enclave with minimal services including a single Root DNS server and NTP services, one at the Brigade Combat Team (BCT) level enclave that sits behind a DMZ as well as a small DODIN enclave with common services. • Traffic generation (TG) will be provided via Mantra and include web and E-mail. The event environment will have 4 ESXi hypervisors, 65 VMs and 40 nodes set up for Traffic Generation using Mantra.		
External Connections: N/A	**Event Classification:** TS/SCI	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Training Event 21-5 will include 5 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 5 weeks of post-event analysis.		

Software Overview

# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name		# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name
1	1		AVG Free		42	42		Mantra
1	1		Adobe Acrobat Reader 9.3		33	33		Meinberg NTP Client
1	1		Adobe Flash Player 10.2 Windows		2	2		Microsoft DNS Server Surrogate Software

1	1		Apache 2.2.15 HTTP Server Linux		2	2		Microsoft Exchange Server 2010 SP2 Enterprise
1	1		Apt Repo		2	2		Microsoft Windows Internet Information Server 2000
2	2		Bind 9.8.1 for Linux		2	2		NTP Server
3	3		CentOS 5.9 x64		6	6		Office 2010
1	1		DHCP Server		1	1		PHP 5.4
2	2		Firewall		6	6		Pidgin
2	2		Network Address Translation		1	1		Putty 0.63
1	1		Windows Fileshare		7	7		RedHat 5.4 x64
1	1		Dovecot		33	33		SSH Server
1	1		Elastic Search		1	1		Ubuntu 12.04 x64
6	6		F Virtual Window Manager		14	14		Vyatta 6.6 x64
18	18		Fedora 16 x86 64		1	1		Webmin 1.760
2	2		GNUPlot		10	10		Windows 2008 R2 SP1
15	15		Gnome Desktop		8	8		Windows 7 Professional SP1 x64
3	3		InspIRCd		1	1		Windows XP Operating System w/SP3
2	2		Domain Controller Surrogate Software		28	28		Yum Repo
7	7		KDE Desktop		3	3		ejabberd XMPP Server
1	1		Kibana		1	1		vsftpd 2.2.2
1	1		Logstash		38	38		wget for Windows

Training Event 21-2		
Description: Training Event 21-2 is a large-scale bi-lateral training event intended to foster collaboration while conducting force-on-force exercise training with significant OPFOR play from robust Red enclaves. It will involve three defensive teams, two different offensive teams and a white cell. For this event, the NCRC has been asked to create an event environment that accurately represents the user's requirements. The even must include a robust Gray environment with realistic internet-level services and elements and real-world threat-representative Blue and Red environments. OPFOR will require robust and detailed Red enclaves to operate from. The event environment for Training Event 21-2 consists of several enclaves as follows: • Backbone Internet Services to include operational instances of all 13 Root DNS servers, domain registration services, NTP and various repos and capabilities, e.g. OS and Yum • The environment will have 3 Regional Internet Grey, 4 Blue and 5 Red enclaves all with sub-enclaves that include different combinations and varieties of Windows and Linux client & server OS and SP configurations, DNS, AD, IIS, Apache, Exchange/Outlook, FTP, SQL databases, live websites, file and video streaming services, etc. Include user provided Hardware-in-the-loop (HWIL) capabilities. Physical routers and firewalls configured IAW "best practices" were added to increase realism and meet specific user requirements. • The user will provide several images that will have to be imported and configured by the NCRC team after which multiple instances will have to be deployed into the event environment. The User has requested specific versions and configurations of some OSs and applications in order to introduce a controlled and known set of vulnerabilities into the exercise. • Traffic generation (TG) will be provided via Mantra and include web, E-mail, fileshare (SMB), and database manipulation modules. The event environment will have 58 ESXi hypervisors, 985 VMs and 625 nodes set up for Traffic Generation using Mantra		
External Connections: JIOR and Joint Mission Environment Test Capability (JMETC) Multiple Independent Levels of Security (MILS) Network (JMN) connections to multiple user locations	**Event Classification:** TS/SCI	**Faraday Cage**: N/A
User Participation: User personnel will not be on site during event execution.	**CSET Participation:** N/A	

Event Timeline: Training Event 21-2 will include 2 months of planning that includes an Initial Planning Conference (IPC), Mid-Planning Conference (MPC) and Final Planning Conference (FPC) of 1-2 days per conference, 4 weeks of range configuration, 2 weeks of event participant network familiarization, 1 week of RECCE, 1 week of event execution and 1 week of post-event activities.

Software Overview

# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name		# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name
80	6		Adobe Acrobat 11.0		17	17		Microsoft Exchange Server 2013 SP1 Enterprise
329	67		Adobe Acrobat Reader 9.3 English Windows Software		142	34		Microsoft Office 2007 Professional Edition w/SP2 Bundled
129	13		Adobe Flash Player 10.2 Windows Software		55	55		Microsoft Windows Internet Information Server 2000
80	6		Adobe Shockwave Player 12.2		89	89		MySQL 5.6
59	59		Apache 2.2.15 HTTP Server Linux		6	2		Office 2003
123	84		Apt Repo		20	2		Office 2010
20	20		Bind 9.8.1 for Linux		253	43		Office 2013
51	51		CentOS (multiple versions)		145	145		PHP 5.4
150	30		Chrome 43.0.2357.65					
19	19		Firewall		1	1		Putty 0.63
3	3		Network Address Translation		514	336		SSH Server
12	12		Windows Fileshare		548	208		SSL Certs
2	2		Domain Registrar Client		1	1		Samba
5	5		Elastic Search		16	16		Security Onion 14.04 x64
1	1		FTP Server		80	6		Silverlight 5.0
422	82		Firefox 35.0.1		2	2		Squid
184	85		Firefox Default for Linux		1	1		SquirrelMail

201	92		Gnome Desktop		2	2		Syslog Server
36	36		Domain Controller Surrogate Software		7	2		Thunderbird 38.0.1
2	2		Secondary Domain Controller		123	84		Ubuntu (multiple versions)
20	2		Internet Explorer 8.0.6001.18702		2	2		Unreal IRCd
80	6		Java SE 8 Update 60 JRE		112	112		VyOS 1.1.6 x64
122	47		Kali 2.0 x64		174	36		Windows 10 Professional SP0
129	50		Kali Linux Full		45	45		Windows 2008 Enterprise SP1 x64
5	5		Kibana		54	54		Windows 2012 R2 Server Update x64
5	5		Logstash		166	40		Windows 3.1 Installer
1002	544		Mantra		87	11		Windows 7 Professional SP1 x64
1003	545		Meinberg NTP Client		1	1		Windows 8.1 Professional x64
20	2		Microsoft .NET Framework 3.5 SP1		41	5		Windows XP Operating System with SP3
18	18		Microsoft .NET Framework 4.5.2		121	31		Windows XP Professional SP2 x64
38	38		Microsoft DHCP Server Surrogate Software		1	1		Wireshark Surrogate Software
36	36		Microsoft DNS Server Surrogate Software		75	75		Yum Repo
19	19		Microsoft Exchange Server 2010 SP2 Enterprise		1096	416		wget for Windows

Test Event 21-6		
Description: Test Event 21-6 is a very complex large-scale event with a primary goal of assessing the security posture of a specific portion of the User's network infrastructure. The NCRC will be deploying a very detailed representation of a portion of the User's real-world networking infrastructure using information and VMs supplied by the User. This event will include traditional penetration testing activities using User supplied tools and data to be performed by NCRC personnel working with User SMEs. • The event environment will consist of a simplified Internet enclave with minimal services including a single Root DNS server and NTP services. There will be a small NIPR representation including HBSS with 2 levels of DMZs that lead to the User provided VMs which are the SUT. The event environment will have 1 ESXi hypervisor, 65 VMs and 40 nodes set up for Traffic Generation using Mantra.		
External Connections: N/A	**Event Classification:** TS/SCI	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Test Event 21-6 will include 6 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 5 weeks of post-event analysis.		

Software Overview							
# of Nodes Containing or Running the SW	**# of Types of Nodes Running the SW**		**Software Application Name**	**# of Nodes Containing or Running the SW**	**# of Types of Nodes Running the SW**		**Software Application Name**
34	5		Adobe Acrobat Reader 9.3	1	1		Microsoft Windows Internet Information Server 2000
34	5		Adobe Flash Player 11.5	1	1		MySQL 5.1
1	1		Bind 9.8.1 for Linux	2	2		PHP 5.4
1	1		CentOS 6.5 x64	2	2		SSH Server
6	6		Firewall	34	5		SSL Certs

34	5		Firefox 35.0.1		3	3		VyOS 1.1.6 x64
4	4		Domain Controller Surrogate Software		11	11		Vyatta 6.6 x64
57	28		Mantra		8	8		Windows 2008 R2 SP1
62	33		Meinberg NTP Client		5	5		Windows 2012 R2 Server Update x64
1	1		Microsoft DHCP Server Surrogate Software		34	5		Windows 7 Professional SP1 x64
4	4		Microsoft DNS Server Surrogate Software		1	1		Yum Repo
2	2		Microsoft Exchange Server 2010 SP2 Enterprise		94	36		wget for Windows
34	5		Microsoft Office 2007 Professional Edition w/SP2 Bundled					

Test Event 21-7		
Description: The primary focus of this complex large-scale test event will be to identify any potential cybersecurity impacts associated integrating a specialized RF sensor into an existing C2 application that had been tested in a previous event. The specialized RF sensor will be operated and stimulated from within the NCRC faraday cage. Both the sensor and C2 application will be provided by the User. This event will include traditional penetration testing activities using User supplied tools and data to be performed by NCRC personnel working with User SMEs. • The event environment will consist of the RF sensor, RF communications and stimulation HW/SW, the sensor C2 application as well as supporting SW and instrumentation. There is no Traffic Generation requirement for this event. The event environment will have 4 ESXi hypervisors and 10 VMs.		
External Connections: N/A	**Event Classification:** TS/SCI	**Faraday Cage**: Required
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Training Event 21-7 will include 5 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 5 weeks of post-event analysis.		

Software Overview							
# of Nodes Containing or Running the SW	**# of Types of Nodes Running the SW**		**Software Application Name**	**# of Nodes Containing or Running the SW**	**# of Types of Nodes Running the SW**		**Software Application Name**
1	1		Apache 2.2.15 HTTP Server Linux	2	2		SSH Server
1	1		Apt Repo	1	1		Ubuntu 12.04 x64
1	1		Elastic Search	1	1		VSFTPD 3.0.2
35	35		Gnome Desktop	1	1		Windows 2008 R2 SP1
35	35		KDE Desktop	35	35		Yum Repo

1	1		Kibana		2	2		wget for Windows
1	1		Logstash		1	1		Apache 2.2.15 HTTP Server Linux
1	1		Mantra		1	1		Apt Repo
37	37		Meinberg NTP Client		1	1		Elastic Search
1	1		PHP Default for Linux		35	35		Gnome Desktop
35	35		RedHat 6.5 x64		2	35		KDE Desktop

Test Event 21-8		
Description: Test Event 21-8 is the latest small-sized event in a series of events that the NCRC has hosted for a Program Office responsible for developing enterprise security solutions for the deployed ground environment. This event will continue the work done during previous events to refine security setting of a solution set prior to be it being formally tested in a Service live-fire event. The PMO intends to provide generated by this event to the Service Operational Test Agency (OTA) as part of the formal testing process. • The event environment will consist of a simplified Internet enclave with minimal services including a single Root DNS server and NTP services, two Blue enclaves, one at the Battalion level and one at the Brigade Combat Team (BCT) level that sit behind a DMZ as well as a small DODIN enclave with common services. • Traffic generation (TG) will be provided via Mantra and include web and email. The event environment will have 1 ESXi hypervisor, 100 VMs and 75 nodes set up for Traffic Generation using Mantra.		
External Connections: N/A	**Event Classification:** Secret	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Test Event 21-8 will include 2 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 2 weeks of post-event analysis.		

Software Overview							
# of Nodes Containing or Running the SW	**# of Types of Nodes Running the SW**		**Software Application Name**	**# of Nodes Containing or Running the SW**	**# of Types of Nodes Running the SW**		**Software Application Name**
90	11		Adobe Acrobat Reader 9.3	3	3		Microsoft Exchange Server 2010 SP2 Enterprise
2	2		Apache 2.2.15 HTTP Server Linux	2	2		Microsoft Windows Internet Information Server 2000
2	2		Apt Repo	4	4		MySQL 5.1

15	15		CentOS (multiple versions)		1	1		NTP Server
2	2		DHCP Server		75	10		Office 2010
2	2		Firewall		13	13		PHP 5.4
1	1		Elastic Search					
100	14		Firefox 35.0.1		4	4		Ubuntu 12.04 x64
3	3		Domain Controller Surrogate Software		10	10		VyOS 1.1.6 x64
8	1		Kali 2017.1		2	1		Windows 2008 Enterprise SP1 x64
1	1		MS SQL Server 2012 Enterprise SP1 x64		17	17		Windows 2008 R2 SP1
100	35		Mantra		75	15		Windows 7 Professional SP1 x64
50	50		Meinberg NTP Client		10	10		Yum Repo
1	1		Microsoft .NET Framework 3.5 SP1		3	3		ejabberd XMPP Server
1	1		DHCP Server Surrogate Software		100	100		wget for Windows
3	3		Microsoft DNS Server Surrogate Software					

Training Event 21-3		
Description: Training Event 21-3 will be the second is a series of "Capture the Flag" style training events where Cyber Protection Teams (CPTs) are able to hone their skills and TTPs in both competitive and non-competitive conditions. This event will have an Army flavor for which the NCRC will provide an event environment replicating 3 different levels of tactical enclaves, i.e. Battalion, Brigade Combat Team (BCT) and Corps, each with 3 different "flags" that teams must find in order to render the unit not mission capable. Each participating team will be given access to an identical environment for a set time period during which they must capture as many 'flags' as possible. • The event environment will consist of a simplified Internet enclave with minimal services including a single Root DNS server and NTP services. A set of Blue enclaves will be provided for each type of tactical enclave that sit behind a DMZ as well as a small DoDIN enclave with common services. • Traffic generation (TG) will be provided via Mantra and include web and email. The event environment will have 2 ESXi hypervisors, 250 VMs and 200 nodes set up for Traffic Generation using Mantra.		
External Connections: JIOR and JMN connections to multiple locations.	**Event Classification:** Secret	**Faraday Cage**: N/A
User Participation: User personnel will not be on site during event execution.	**CSET Participation:** N/A	
Event Timeline: Training Event 21-3 will include 6 weeks of planning, 2 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 2 weeks of post-event analysis.		

Software Overview							
# of Nodes Containing or Running the SW	**# of Types of Nodes Running the SW**		**Software Application Name**	**# of Nodes Containing or Running the SW**	**# of Types of Nodes Running the SW**		**Software Application Name**
180	22		Adobe Acrobat Reader 9.3	5	5		Microsoft DNS Server Surrogate Software
3	3		Apache 2.2.15 HTTP Server Linux	5	5		Microsoft Exchange Server 2010 SP2 Enterprise

4	4		Apt Repo		5	5		Microsoft Windows Internet Information Server 2000
1	1		Bind 9.8.1 for Linux		8	8		MySQL 5.1
32	32		CentOS (multiple versions)		1	1		NTP Server
4	4		DHCP Server		180	22		Office 2010
4	4		Firewall		13	13		PHP 5.4
1	1		Elastic Search		188	23		Pidgin
188	23		Firefox 35.0.1		28	14		SSH Server
5	5		Domain Controller Surrogate Software		2	2		Samba
16	2		Kali 2017.1		4	4		Ubuntu 12.04 x64
1	1		Kibana		18	18		VyOS 1.1.6 x64
1	1		Logstash		4	1		Windows 2008 Enterprise SP1 x64
1	1		MS SQL Server 2012 Enterprise SP1 x64		17	17		Windows 2008 R2 SP1
237	72		Mantra		180	22		Windows 7 Professional SP1 x64
62	55		Meinberg NTP Client		32	32		Yum Repo
2	2		Microsoft .NET Framework 3.5 SP1		3	3		ejabberd XMPP Server
1	1		DHCP Server Surrogate Software		402	80		wget for Windows

Test Event 21-9		
Description: Test Event 21-9 is the initial small-sized event the NCRC will host for a Program Office responsible for developing methodologies and solutions for assessing the security posture of contractors supporting development of security solutions that are intended for deployment within DoD garrison environments. The intent is to develop solutions and methodologies that can be rapidly applied to improve the overall cybersecurity posture of the DIB. The event will include a cooperative vulnerability assessment and traditional penetration testing activities. • The event environment will consist of a small Internet enclave and an internal enclave behind a DMZ with sub-enclaves for 2 generalized garrison enclaves and a single building enclave to house the SUT. The User will provide the SUT solutions that are to be tested as well as SME support as needed. The event environment will have3 ESXi hypervisors and 50 nodes set up for Traffic Generation using Mantra.		
External Connections: N/A	**Event Classification:** Unclassified	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Test Event 21-9 will include 3 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 2 weeks of post-event analysis.		

Software Overview							
# of Nodes Containing or Running the SW	**# of Types of Nodes Running the SW**		**Software Application Name**	**# of Nodes Containing or Running the SW**	**# of Types of Nodes Running the SW**		**Software Application Name**
50	3		Adobe Acrobat Reader 9.3	2	2		Microsoft DNS Server Surrogate
50	3		Adobe Flash Player 11.5	2	2		Microsoft Exchange Server 2010 SP2 Enterprise
1	1		Apache 2.2.15 HTTP Server Linux	50	3		Microsoft Office 2007 Professional SP2
2	2		Apt Repo	1	1		PHP Default for Linux

1	1		Firewall		15	15		SSH Server
2	2		Windows Fileshare		1	1		Syslog Client
1	1		Elastic Search		1	1		Syslog Server
2	2		Domain Controller Surrogate		2	2		Ubuntu 12.04 x64
7	7		Kali 2.0 x64		5	5		Vyatta 6.6 x64
7	7		Kali Linux Full		1	1		Windows 2000 Server SP4 x86
1	1		Kibana		1	1		Windows 2003 Enterprise SP2 x86
1	1		Logstash		8	8		Windows 2008 R2 SP1
1	1		MS SQL Server 2012 Enterprise SP1 x64		1	1		Windows 2012 R2 Server x64
72	25		Mantra		54	7		Windows 7 Enterprise SP1 x64
1	1		Meinberg NTP Client		2	2		Windows XP Professional SP2 x64
2	2		Microsoft DHCP Server Surrogate		130	36		wget for Windows

Test Event 21-10		
Description: Test Event 21-10 will evaluate the effectiveness and suitability of a User developed and supplied capability prior to it being deployed in support of real-world operations. The capability must be tested within the context of the Government user requirements in a realistic environment. This event will include traditional penetration testing activities using User supplied tools and data to be performed by NCRC personnel working with User SMEs. The four components of the environment will be: • A robust Internet Backbone enclave to include operational instances of all 13 Root DNS servers, domain registration services and NTP, 30 distinct Grey enclaves with regional distinctions that host numerous and different configurations of functional Content Management System (CMS) sites along with numerous non-CMS functional websites • A Capability Enclave used to host the User provided SUT • A dedicated Traffic Generation enclave using Mantra for web (HTTP and HTTPS) traffic that interacts with the CMS and other web services in the internet enclave. The event environment will have 15 ESXi hypervisors, 750 VMs and 1 node set up to support Mantra Traffic Generation		
External Connections: N/A	**Event Classification:** TS/SCI	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Test Event 21-10 will include 4 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 5 weeks of post-event analysis.		

Software Overview

# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name		# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name
102	102		Apache 2.2.15 HTTP Server Linux		270	270		SSH Server
26	26		Apt Repo		21	21		Ubuntu 14.04 x86

1	1		Bind 9.8.1 for Linux		3	3		VyOS 1.1.6 x64
112	93		CentOS 7.0 x64		27	27		Vyatta 6.6 x64
5	5		Debian 7.8 x64		8	8		Website Module Drupal
1	1		Elastic Search		7	7		Website Module MyBB
64	7		Firefox 35.0.1		8	8		Website Module Phpbb
24	24		Gnome Desktop		9	9		Website Module SMF
1	1		Kibana		10	10		Website Module WordPress
1	1		Logstash		9	9		Website Module vBulletin
198	141		Mantra		20	1		Windows 7 Professional SP1 x64
51	51		MySQL Default		20	1		Windows 8.1 x64
36	36		Microsoft DNS Server Surrogate Software		112	93		Yum Repo
167	167		PHP Default for Linux		80	4		wget for Windows

Test Event 21-11		
Description: Test Event 21-11 will be a large-scale test event focused on evaluating the suitability and usability of a newly developed capability for supporting data collection and analysis during testing and training events. The SUT is very complex and will require significant effort to instantiate on the range. The event environment for this test will be highly instrumented with non-interfering sensors and have significant data collection requirements. The SUT will be hosted by the NCRC and will be largely virtualized with a small number of physical hosts being required. The event environment will consist of the following enclaves: • A small Internet backbone with an operational instance of a Root DNS server and an NTP service • A number of Blue, Red and Grey enclaves with sub-enclaves that include different combinations and varieties of Windows and Linux client & server OS and SP configurations as well as Exchange/Outlook E-mail, File Sharing, Chat, websites, in-game Voice Over Internet Protocol (VOIP) telephony services will be provided using Cisco routing hardware The event environment will have 10 ESXi hypervisors, 682 VMs and 344 nodes set up for Traffic Generation using Mantra.		
External Connections: N/A	**Event Classification:** TS/SCI	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** N/A	
Event Timeline: Test Event 21-11 will include 6 weeks of planning that includes 2 technical exchanges of 2-3 days each with the User, includes 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 6 weeks of post-event analysis.		

Software Overview

# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name		# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name
341	85		Adobe Acrobat Reader 9.3 English Windows Software		41	41		Microsoft Windows Internet Information Server 2000
129	53		Adobe Flash Player 11.5		14	14		MySQL 5.6

63	63		Apache 2.2.15 HTTP Server Linux		66	66		MySQL Default
5	5		Apt Repo		1	1		NTP Server
1	1		Asterisk 11.5.1 for Linux		260	71		Office 2010
8	8		Bind 9.8.1 for Linux		137	137		PHP Default for Linux
85	85		CentOS (multiple versions)		10	1		Pidgin
200	20		Chrome 43.0.2357.65		233	225		SSH Server
34	34		Firewalls		331	84		SSL Certs
6	6		Windows Fileshare		1	1		Samba
872	360		DOS 6.22 Windows		5	5		Security Onion 14.04 x64
1	1		Dovecot		1	1		Squid
1	1		Elastic Search		1	1		SquirrelMail
6	6		Fedora 16 x86		5	5		Ubuntu 12.04 x64
342	86		Firefox 35.0.1		123	123		VyOS 1.1.6 x64
25	17		Gnome Desktop		4	4		Windows 10 Professional v1511 SP0
30	30		Domain Controller Surrogate Software		1	1		Windows 2003 Enterprise SP2 x86
22	14		Kali 2.0 x64		74	74		Windows 2008 R2 SP1
1	1		Kibana		10	10		Windows 2012 Server x86 64
1	1		Logstash		3	3		Windows 3.1 Installer
682	418		Mantra		331	75		Windows 7 Professional SP1 x64
246	238		Meinberg NTP Client		60	6		Windows 7 Professional SP1 x86
26	26		Microsoft DHCP Server Surrogate Software		4	4		Windows Vista Enterprise Operating System
38	38		Microsoft DNS Server Surrogate Software		2	2		Windows XP Professional SP2 x86
29	29		Microsoft Exchange Server 2010 SP2 Enterprise		91	91		Yum Repo

5	5		Microsoft Exchange Server 2013 SP1 Enterprise		2	2		ejabberd XMPP Server
81	14		Microsoft Office 2007 Professional Edition w/SP2 Bundled		872	360		wget for Windows

Test Event 21-2.2		
Description: Test Event 21-2.2 is the second in a series of large-scale test events that will independently test and evaluate commercial Industrial Control System (ICS) technologies and products and how they might be applied and integrated in analogous DoD systems. The event will include a cooperative vulnerability assessment and traditional penetration testing activities. • The event environment will consist of a small Internet enclave and an internal enclave behind a DMZ with sub-enclaves for 2 control enclaves and a building enclave that acts as the SUT. The User will provide the commercial products that are to be tested and the vendors will provide technical assistance as needed for their products. The event environment will have no hypervisors and 54 nodes set up for Traffic Generation using Mantra.		
External Connections: N/A	**Event Classification:** Secret	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Test Event 21-2.2 will include 3 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 2 weeks of post-event analysis.		

Software Overview

# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name		# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name
50	3		Adobe Acrobat Reader 9.3		2	2		Microsoft DNS Server Surrogate
50	3		Adobe Flash Player 11.5		2	2		Microsoft Exchange Server 2010 SP2 Enterprise
1	1		Apache 2.2.15 HTTP Server Linux		50	3		Microsoft Office 2007 Professional SP2
2	2		Apt Repo		1	1		PHP Default for Linux

1	1		Firewall		15	15		SSH Server
2	2		Windows Fileshare		1	1		Syslog Client
1	1		Elastic Search		1	1		Syslog Server
2	2		Domain Controller Surrogate		2	2		Ubuntu 12.04 x64
7	7		Kali 2.0 x64		5	5		Vyatta 6.6 x64
7	7		Kali Linux Full		1	1		Windows 2000 Server SP4 x86
1	1		Kibana		1	1		Windows 2003 Enterprise SP2 x86
1	1		Logstash		8	8		Windows 2008 R2 SP1
1	1		MS SQL Server 2012 Enterprise SP1 x64		1	1		Windows 2012 R2 Server x64
72	25		Mantra		54	7		Windows 7 Enterprise SP1 x64
1	1		Meinberg NTP Client		2	2		Windows XP Professional SP2 x64
2	2		Microsoft DHCP Server Surrogate		130	36		wget for Windows

Training Event 21-4		
Description: Training Event 21-4 will be a medium sized Command Post Exercise (CPX) level exercise centered on information dissemination operations that is being used to prepare for an upcoming Service level exercise. Exercise participants will be connected to the NCRC-provided environment remotely using the Joint Information Operations Range (JIOR). The event environment will include: • A robust Internet Backbone enclave to include operational instances of all 13 Root DNS servers, domain registration services and NTP, 3 regionally distinct Grey enclaves that host numerous and different configurations of functional Content Management System (CMS) sites along with numerous non-CMS functional websites and 2 Blue enclaves from which the event participants will access the environment. • Extensive traffic Generation using Mantra for web (HTTP and HTTPS) traffic that interacts with the CMS and other web services in the Internet enclave. The event environment will have 15 ESXi hypervisors, 600 VMs and 45 nodes set up to support Mantra Traffic Generation		
External Connections: JIOR connections to multiple locations	**Event Classification:** Secret	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** N/A	
Event Timeline: Training Event 21-4 will include 5 weeks of planning, 3 weeks of range configuration, 1 week of event execution, 1 week of post-event activities and 3 weeks of post-event analysis.		

Software Overview							
# of Nodes Containing or Running the SW	**# of Types of Nodes Running the SW**		**Software Application Name**	**# of Nodes Containing or Running the SW**	**# of Types of Nodes Running the SW**		**Software Application Name**
198	24		Adobe Acrobat Reader 9.3	42	270		Pidgin
47	47		Apache 2.2.15 HTTP Server Linux	9	21		RedHat 6.4 x64
107	35		Apt Repo	117	3		SSH Server

14	14		Bind 9.8.1 for Linux		82	27		SSL Certs
43	43		CentOS 6.5 x64		1	8		Samba
198	24		Chrome 43.0.2357.65		23	7		Ubuntu 12.04 x64
21	21		Firewall		1	8		VSFTPD 3.0.2
84	12		Debian 7.8 x64		76	9		VyOS 1.1.6 x64
1	1		Domain Registrar Client		1	10		Website Module domain registrar
1	1		Elastic Search		1			Website Module drupal
359	48		Firefox 35.0.1		1			Website Module mybb
155	29		Gnome Desktop		1			Website Module ncr dynamic
24	24		Domain Controller Surrogate Software		1			Website Module phpbb
1	1		Kibana		1			Website Module vbulletin
1	1		Logstash		1			Website Module wordpress
501	228		Mantra		2			Website Module wordpress theme site
290	164		Meinberg NTP Client		27			Windows 2008 R2 Ent SP0 x64
24	24		Microsoft DHCP Server Surrogate Software		30			Windows 2008 R2 SP1
24	24		Microsoft DNS Server Surrogate Software		1			Windows 2012 R2 Server x64
24	24		Microsoft Exchange Server 2010 SP2 Enterprise		24			Windows 7 Professional SP1 x64
30	30		Microsoft Windows Internet Information Server 2000		52			Yum Repo
50	50		MySQL 5.1		3	9		ejabberd XMPP Server
1	1		NTP Server		17	1		socat
198	24		Office 2010		1	1		vsftpd 2.2.2
9	9		PHP 5.4		164	93		wget for Windows
52	52		PHP Default for Linux					

Test Event 21-12		
Description: Test Event 21-12 is a medium-scale test event that will evaluate and compare two proposed security solutions that are being considered for integration into an already fielded system. The User will be providing the SUTs as well as SME engineering support during the event execution. This event will include traditional penetration testing activities using User supplied tools and data to be performed by NCRC personnel working with User SMEs. The event will include a cooperative vulnerability assessment of each proposed solution. • The event environment will consist of a small Internet enclave and an internal enclave behind a DMZ with a sub-enclave to host the SUT. The event environment will have 2 ESXi hypervisors, 10 VMs and 25 nodes for Traffic Generation using Mantra.		
External Connections: N/A	**Event Classification:** Secret	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Test Event 21-12 will include 3 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 3 weeks of post-event analysis.		

Software Overview

# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name		# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name
1	1		Apache 2.2.15 HTTP Server Linux		1	1		Logstash
12	3		Apt Repo		35	26		Mantra
2	2		CentOS 7.0 x64		1	1		Meinberg NTP Client
1	1		Chrome 43.0.2357.65		1	1		PHP Default for Linux
4	4		Firewall		35	26		SSH Server

1	1		Elastic Search		12	11		Ubuntu 12.04 x64
10	1		FTP Server		9	9		VyOS 1.1.6 x64
3	3		Firefox 35.0.1		11	11		Windows 7 Professional SP1 x64
13	4		Gnome Desktop		1	1		Wireshark 2.0.3 for Windows
10	10		Kali 2.0 x64		2	2		Yum Repo
1	1		Kibana		22	22		wget for Windows

Test Event 21-13

Description: Test Event 21-13 is the first event that the NCRC will host for a Program Office responsible for developing software for centrally managing High Assurance Guards (HAGs). This small event will be an initial risk-reduction event with the objective of hosting the PMO provided application VMs on a small-scale representative network infrastructure. This event will not include a cooperative vulnerability assessment and traditional penetration testing activities.

- The event environment will consist of 4 small unit level enclaves connected across a small-scale representation of the DODIN backbone. IAP/JRSS is not required for this event. The User will provide the SUT software as well as SME support as needed.

The event environment will have 2 ESXi hypervisors and no Traffic Generation.

External Connections: N/A	**Event Classification:** TS/SCI	**Faraday Cage**: N/A

User Participation: User personnel will be on site during event execution.	**CSET Participation:** N/A

Event Timeline: Test Event 21-13 will include 3 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 2 weeks of post-event analysis.

Software Overview

# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name		# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name
1	1		Apache 2.2.15 HTTP Server Linux		2	2		Microsoft DNS Server Surrogate
					2	2		Microsoft Exchange Server 2010 SP2 Enterprise
1	1		Firewall		50	3		Microsoft Office 2007 Professional SP2
2	2		Windows Fileshare		1	1		PHP Default for Linux
1	1		Elastic Search		2	2		Ubuntu 12.04 x64

2	2		Domain Controller Surrogate		5	5		Vyatta 6.6 x64
7	7		Kali 2.0 x64		1	1		Windows 2000 Server SP4 x86
7	7		Kali Linux Full		1	1		Windows 2003 Enterprise SP2 x86
1	1		Kibana		8	8		Windows 2008 R2 SP1
1	1		Logstash		1	1		Windows 2012 R2 Server x64
1	1		MS SQL Server 2012 Enterprise SP1 x64		54	7		Windows 7 Enterprise SP1 x64
1	1		Meinberg NTP Client		2	2		Windows XP Professional SP2 x64
2	2		Microsoft DHCP Server Surrogate					

Training Event 21-5		
Description: Training Event 21-5 is a large-scale event to conduct force-on-force training of the Cyber Mission Force (CMF). It will involve two defensive teams, an offensive team and a white cell. For this event, the NCRC has been asked to create an event environment that accurately represents the user's requirements. The even must include a robust Gray environment with realistic internet-level services and elements and real-world representative Blue and Red environments that allow Blue player to exercise their TTPs and MESLs. The event environment will consist of several enclaves as follows: • Backbone Internet Services to include operational instances of all 13 Root DNS servers, domain registration services, NTP and various repos and capabilities, e.g. OS, Phython (PyPI), PyCharm • The environment will have 3 Regional Internet Grey, 4 Blue and 5 Red enclaves all with sub-enclaves that include different combinations and varieties of Windows and Linux client & server OS and SP configurations, DNS, AD, IIS, Tomcat, Apache, Exchange/Outlook, FTP, SQL databases, live websites, file and video streaming services, etc. The event environment will have 51 ESXi hypervisors, 758 VMs and 522 nodes set up for Traffic Generation using Mantra.		
External Connections: JIOR & JMN connections to multiple user locations	**Event Classification:** TS/SCI	**Faraday Cage**: N/A
User Participation: User personnel will not be on site during event execution.	**CSET Participation:** N/A	
Event Timeline: Training Event 21-5 will include 2 months of planning that includes IPC, MPC and FPC of 1-2 days per conference, 4 weeks of range configuration, 2 weeks of event participant network familiarization, 1 week of RECCE, 1 week of event execution and 2 weeks of post-event activities.		

Software Overview							
# of Nodes Containing or Running the SW	**# of Types of Nodes Running the SW**		**Software Application Name**		**# of Nodes Containing or Running the SW**	**# of Types of Nodes Running the SW**	**Software Application Name**
112	30		7-Zip 9.20		21	21	Microsoft DHCP Server Surrogate Software

140	38		Adobe Acrobat 11.0		23	23		Microsoft DNS Server Surrogate Software
37	37		Apache 2.2.15 HTTP Server Linux		25	25		Microsoft Exchange Server 2010 SP2 Enterprise
132	47		Apt Repo		41	41		Microsoft Windows IIS Server 2000
15	15		Bind 9.8.1 Linux		12	12		MySQL (multiple versions)
31	31		CentOS (multiple versions)		137	39		Notepad++ 5.8.2
220	37		Chrome (multiple versions)		180	25		Office 2010
26	26		Firewall		135	37		Office 2010 Pro SP2 x86
2	2		Network Address Translation		56	56		PHP 5.4
84	12		Debian 7.8 x64		135	37		Powershell 5.1
2	2		Domain Registrar Client		77	27		Putty 0.63
1	1		Elastic Search		135	37		Python 2.7
120	32		Fiddler 4.6		63	9		RedHat (multiple versions)
120	32		FileZilla		176	131		SSH Server
408	70		Firefox (multiple versions)		168	21		SSL Certs
174	35		Gnome_Desktop		5	3		Samba
23	23		Domain Controller Surrogate		35	35		Ubuntu (multiple versions)
140	38		Java SE 6		135	37		VLC Player 2.2.6
5	1		Kali 2.0 x64		85	85		VyOS 1.1.6 x64
26	22		Kali 2017.1		181	71		WSUS Client
31	23		Kali Linux Full		117	31		WinRAR 5.5 Beta 6
1	1		Kibana		21	21		Windows 2008 R2 Ent SP0 x64
1	1		Logstash		32	32		Windows 2008 R2 SP1
754	348		Mantra		1	1		Windows 2012 R2 Server x64
355	206		Meinberg NTP Client		168	21		Windows 7 Professional SP1 x64
140	38		Microsoft .NET Framework 3.5 SP1		107	51		Yum Repo

Test Event 21-2.3		
Description: Test Event 21-2.3 is the third in a series of large-scale test events that will independently test and evaluate commercial Industrial Control System (ICS) technologies and products and how they might be applied and integrated in analogous DoD systems. The event will include a cooperative vulnerability assessment and traditional penetration testing activities. • The event environment will consist of a small Internet enclave and an internal enclave behind a DMZ with sub-enclaves for 2 control enclaves and a building enclave that acts as the SUT. The User will provide the commercial products that are to be tested and the vendors will provide technical assistance as needed for their products. The event environment will have no hypervisors and 54 nodes set up for Traffic Generation using Mantra.		
External Connections: N/A	**Event Classification:** Secret	**Faraday Cage**: N/A
User Participation: User personnel will be on site during event execution.	**CSET Participation:** Required	
Event Timeline: Test Event 21-2.3 will include 6 weeks of planning, 3 weeks of range configuration, 2 weeks of event execution, 1 week of post-event activities and 3 weeks of post-event analysis.		

Software Overview

# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name		# of Nodes Containing or Running the SW	# of Types of Nodes Running the SW		Software Application Name
50	3		Adobe Acrobat Reader 9.3		2	2		Microsoft DNS Server Surrogate
50	3		Adobe Flash Player 11.5		2	2		Microsoft Exchange Server 2010 SP2 Enterprise
1	1		Apache 2.2.15 HTTP Server Linux		50	3		Microsoft Office 2007 Professional SP2

2	2		Apt Repo		1	1		PHP Default for Linux
1	1		Firewall		15	15		SSH Server
2	2		Windows Fileshare		1	1		Syslog Client
1	1		Elastic Search		1	1		Syslog Server
2	2		Domain Controller Surrogate		2	2		Ubuntu 12.04 x64
7	7		Kali 2.0 x64		5	5		Vyatta 6.6 x64
7	7		Kali Linux Full		1	1		Windows 2000 Server SP4 x86
1	1		Kibana		1	1		Windows 2003 Enterprise SP2 x86
1	1		Logstash		8	8		Windows 2008 R2 SP1
1	1		MS SQL Server 2012 Enterprise SP1 x64		1	1		Windows 2012 R2 Server x64
72	25		Mantra		54	7		Windows 7 Enterprise SP1 x64
1	1		Meinberg NTP Client		2	2		Windows XP Professional SP2 x64
2	2		Microsoft DHCP Server Surrogate		130	36		wget for Windows