INSTITUTE FOR DEFENSE ANALYSES

Assessment of the Cybersecurity Developmental Test Cross-Service Working Group and Recommendations for Improvement

Dr. Rachel Kuzio de Naray
Ms. Allison J. Savoy-Logan

August 2023
IDA Publication D-33585
Log: H 2023-000260
ANDREW report 3000545

Cleared for Public Release by the DoD Office of Prepublication Review, Case 24-T-0072, 11 October 2023

INSTITUTE FOR DEFENSE ANALYSES 730
East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project AX-01-3100, "Technical Analysis for the Director, Developmental Test, Evaluation, and Assessments," for the Director, Developmental Test Evaluation and Assessments. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Cleared for Public Release by the DoD Office of Prepublication Review, Case 24-T-0072, 11 October 2023

Acknowledgments

The authors would like to thank the IDA review committee, Dr. Stephen Ouellette (chair), Dr. Jaikrishna Venkatesan, Dr. Patrick J. Jaffke, and Dr. Jason R. Schlup for providing technical review of this effort.

For More Information

Rachel Kuzio de Naray, Project Leader
rdenaray@ida.org, 703-933-6556

Stephen M. Ouellette Director, SED
souellet@ida.org, (703) 845-2443

Rigorous Analysis | Trusted Expertise | Service to the Nation

I N S T I T U T E F O R D E F E N S E A N A L Y S E S

IDA Document D-33585

Assessment of the Cybersecurity Developmental Test Cross-Service Working Group and Recommendations for Improvement

Dr. Rachel Kuzio de Naray
Ms. Allison J. Savoy-Logan

Executive Summary

The Cybersecurity Developmental Test Cross-Service Working Group (CyberDT XSWG) is a community that formed in 2016 to support and champion the needs of cyber developmental test and evaluation (DT&E) professionals. Its stated mission is to promote collaboration and knowledge sharing between Service and Agency cyber DT&E organizations, develop cyber DT&E best practices, and enhance cyber DT&E capability and influence within Defense Acquisition processes.

This document reviews the history of CyberDT XSWG activities and initiatives, post-event surveys completed by the working group (WG) members, and the results of a self-assessment conducted by CyberDT XSWG leadership. The gathered information will help to evaluate the extent to which the CyberDT XSWG is meeting its objectives. Recommended actions that would improve the execution of the CyberDT XSWG mission are provided.

Overall, the CyberDT XSWG is meeting or partially meeting all of its stated mission and carries out nearly all activities listed in its charter. It has grown in membership, expanded and spawned new activities, collaborations and partnerships, and been responsive to the needs of the community. In particular, the WG excels at providing opportunities for learning and networking.

Nevertheless, there is room for the CyberDT XSWG to grow in achieving its objective of providing improved access to cyber intelligence. Equally beneficial would be the development of yearly goals and a formal roadmap to achieving those goals by the CyberDT XSWG leadership. Increasing the visibility of the CyberDT XSWG leadership will elevate the voices of the WG membership, as the members will know who to contact to advocate for their needs. Progress in these three areas would have the most impact on ensuring the continued success of the CyberDT XSWG.

Contents

Tables

Figures

1. Background

The Cybersecurity Developmental Test Cross-Service Working Group (CyberDT XSWG) is a community formed to support and champion the needs of Service and Agency cyber developmental test and evaluation (DT&E) professionals (see Figure 1-1). The following sections describe the creation of the working group (WG), its mission, membership, structure, and activities.

Figure 1-1. The CyberDT XSWG logo and objective

A. Creation

The CyberDT XSWG originated from the findings and recommendations of a 2016 Institute for Defense Analyses (IDA) report characterizing the capability and capacity of the DoD Cybersecurity Developmental Test and Evaluation enterprise. [1] This report discussed various gaps in DoD Cybersecurity T&E, with one of the gap areas related to the coordination of resources. The discussions with the Services and Agencies revealed the existence of duplicative infrastructure and tools, as well as other issues that could potentially be resolved by leveraging shared resources. To address this gap, it was suggested that "regular forums could be stood up to facilitate organizations' sharing of tools, practices, techniques, and testing observations that could allow for natural connections and coordination efforts to arise." [1]

Motivated by these findings, the sponsor of that report, the Cybersecurity/Interoperability Technical Director in the Office of the Under Secretary of Defense for Research & Engineering, Developmental Test and Evaluation (OUSD R&E, DT&E[1]) initiated discussions with Air Force, Army, and Navy T&E executives to propose the idea of a cross-service working group and gain their buy-in and support. The inaugural

[1] DT&E is now Developmental Test, Evaluation, and Assessments (DTE&A).

CyberDT XSWG event, CyberDT XSWG-01, was subsequently hosted by the Army at White Sands Missile Range (WSMR) in October 2016. The charter for the WG was formalized eight months later, in June 2017.

B. Mission

The CyberDT XSWG Charter formally documents the (1) purpose, (2) goals/objectives, (3) organizational structure, including identifying the participants, responsibilities of the Senior Stakeholder Board (SSB), and decision-making/change management, (4) activities, and (5) communication methods of the group. Though the Charter is regularly revised to reflect changes in the membership of the SSB, the only substantive change since V1.0 was the addition in V1.1 (March 2020) of a "Yearly Goals" activity. The text of sections (1) and (2), and portions of section (4) in V1.14 (approved 24 May 2023) are reproduced below to provide a description of the intended role of the CyberDT XSWG. [2]

1. Charter Section 1: Working Group Purpose

> *To enhance collaboration and knowledge sharing between the Service and Agency Cybersecurity Developmental Test Organizations to further improve Cybersecurity Developmental Test and Evaluation in DoD programs.*
>
> ***Promote –*** *Collaboration and knowledge sharing between Service and Agency Cyber DT&E Organizations.*
>
> ***Develop –*** *Cyber DT&E best practices for application to Defense Acquisition.*
>
> ***Enhance –*** *Cyber DT&E capability and influence within the Defense Acquisition processes securing both improvements in efficacy and efficiency.*

2. Charter Section 2: Goals/Objectives

> *Provide a recurring forum for Cybersecurity Test Teams to:*
>
> - ***(Promote)*** *Identify and disseminate lessons learned, results from internal research, and other subject matter expertise across the Test Teams.*

- ***(Promote)*** *Identify opportunities for sharing of lessons learned and collaborative development of techniques, tools, CONOPs, analysis, metrics, reporting methodologies, and other best practices.*
- ***(Develop)*** *Provide targeted training opportunities for Test Team personnel.*
- ***(Develop)*** *Provide an active and engaged forum for policy feedback and development; promulgate the latest policy and guidance to the Cyber DT&E professionals.*
- ***(Enhance)*** *Streamline the flow of current cyber intelligence information to Testers to assure timely application to system design.*
- ***(Enhance)*** *Identify, implement, and develop measures of efficacy and efficiency related to Cyber DT&E implementation.*

3. Charter Section 4: Activities

Principle activity is a biannual WG meeting:

- *Hosting duties will rotate among the organizations represented by the SSB.*
- *Target is 1-2 day meeting with presentations from each organization of their choosing.*

Additional Activities:

- *The goal is to meet the needs of the community and to create change where possible. As such, other potential activities may be involved such as, but not limited to:*
    - *Breakout sessions on specific topics … with output products.*
    - *Initiation of ongoing ad hoc projects or sub-working group as a byproduct of the XSWG effort.*
    - *Specialized technical training for the technical operators/cyber analysts.*
- *Identification of "Yearly Goals" for addressing high-priority future T&E challenges:*

- *Identification of specific actions the XSWG can take to support, advance, or answer the cyber-related challenges faced by the T&E community.*

C. Membership

As stated in the Charter, the purpose of the CyberDT XSWG is to bring together Service and Agency Cybersecurity Developmental Test Organizations. As such, the Key Organizations identified in the Charter[2] include [2]:

- **Army:** Army Research Lab (ARL)/Combat Capabilities Development Command (DEVCOM) Analysis Center (DAC); Army Test and Evaluation Command (ATEC)
- **Air Force:** 48th Cyber Test Squadron (CTS); Air Force Test and Evaluation (AF/TE); Air Force Materiel Command (AFMC)
- **Marine Corps:** Marine Corps Systems Command (MARCORSYSCOM); Marine Corps Tactical Systems Support Activity (MCTSSA)
- **Navy:** Naval Air Systems Command (NAVAIR); Naval Sea Systems Command (NAVSEA); Naval Information Warfare Center Pacific (NIWC PAC); Navy Test and Evaluation (OPNAV N94)
- **US Space Force:** Space Force Test and Evaluation (USSF/TE)
- **US Coast Guard**
- **Defense Information Systems Agency (DISA)**
- **Joint Interoperability Test Command (JITC)**
- **Missile Defense Agency (MDA)**
- **Office of the Secretary of Defense (OSD):** Executive Director, Developmental Test, Evaluation, and Assessments (ED,DTE&A); Director, Operational Test and Evaluation (DOT&E); OUSD R&E, Strategic Technology Protection and Exploitation (STP&E); Test Resource Management Center (TRMC); DoD Chief Information Officer (CIO)
- **Intel:** Defense Intelligence Agency (DIA); National Air and Space Intel Center (NASIC); National Ground Intelligence Center (NGIC); Office of Naval Intelligence (ONI)
- **Department of Homeland Security (DHS)**

[2] Note that the list of Key Organizations is as it appears in the Charter; some organizations have been renamed, and others might be more appropriately listed in a different group.

- **Operational Test Agencies (OTAs):** Air Force Operational Test and Evaluation Center (AFOTEC); Army Threat Systems Management Office (TSMO); Navy Commander Operational Test and Evaluation Force (COMOPTEVFOR/COTF); Marine Corps Operational Test and Evaluation Activity (MCOTEA)

As of mid-April 2023, the CyberDT XSWG roster has nearly 600 members; roughly 150 of these members are a consistently active "core group." As seen in Figure 1-2, over 75 percent of the membership comes from the Navy, Army, Air Force and OSD groups. In addition to members from these Key Organizations, individuals from Federally Funded Research and Development Centers (FFRDCs) and University Affiliated Research Centers (UARCs) are also members of the CyberDT XSWG. There is a small fraction of individuals from commercial companies, but they are only admitted to the WG if they are directly and currently supporting a T&E organization.

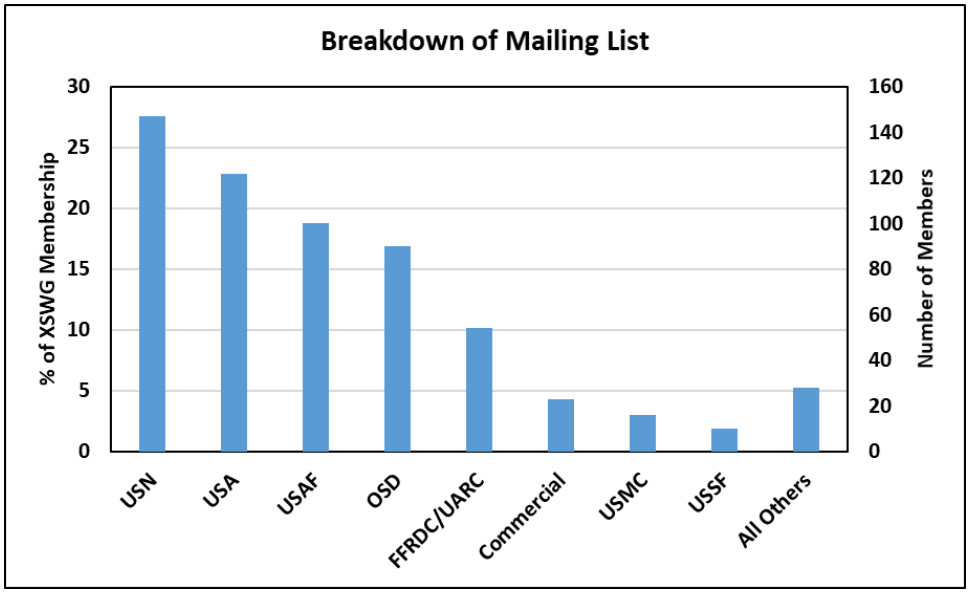


Figure 1-2. Distribution of CyberDT XSWG membership as of mid-April 2023

D. Leadership

The leaders of the CyberDT XSWG are the Senior Stakeholder Board (SSB) members who "establish direction, set priorities, monitor WG meeting planning, provide approvals, and ensure equitable participation opportunities among organizations involved." [2] The current[3] SSB members are:

[3] Current as of July 2023.

- **OUSD R&E, DDTE&A:** Sarah Standard, Cybersecurity/Interoperability Technical Director
- **USN:** Karl Glaeser, OPNAV N942; Stephanie Moffite, OPNAV N942
- **USA:** Brian Flaherty, DUSA-TE; Dan Landin, DEVCOM DAC
- **USAF:** Jim Hobin, 48th CTS; Max Rogozinski, AF/TE
- **USMC:** Shawn Stone, MCTSSA
- **TRMC:** Robert Tamburello, Deputy Executive Agent for DoD Cyber Test Ranges
- **USSF:** Lt Col Michael Christensen, USSF/TE

E. IDA's Role and Responsibilities

Though not officially part of the SSB, IDA works closely with the CyberDT XSWG leadership team to identify and recommend relevant topics and/or activities for the WG to pursue, maintain institutional knowledge as individual SSB members rotate out, and assist with organizing and facilitating WG activities. Additionally, as discussed in subsequent sections, IDA maintains the communications mechanisms/platforms for the WG, and distributes and analyzes post-event surveys to collect feedback from the membership.

F. Avenues of Communication

The CyberDT XSWG has two main mechanisms/platforms for communication: email and Intelink SharePoint pages.

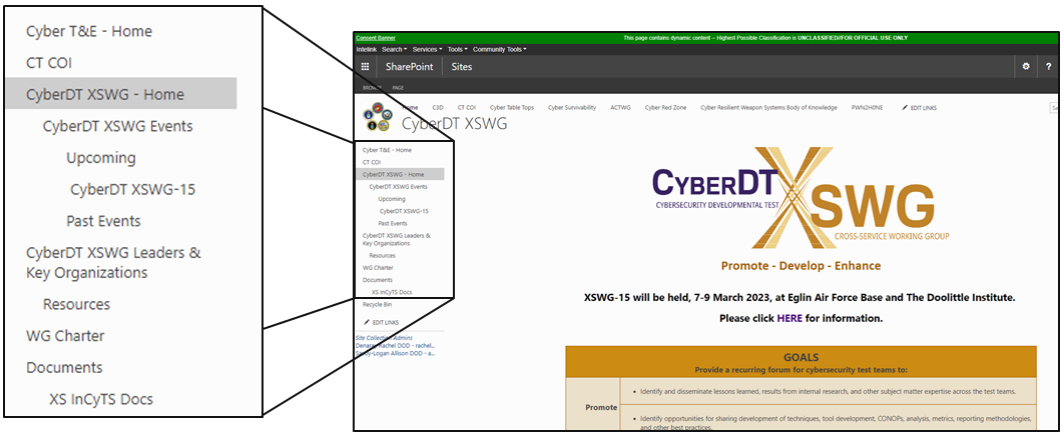
The mailing list is used for sending announcements and invitations. Any member of the cyber T&E community can request to be added to the list; members can also request to be removed at any time. The mailing list is maintained by IDA and periodically scrubbed by the SSB.

The CyberDT XSWG has both unclassified[4] and classified[5] (i.e., Secure Internet Protocol Router Network (SIPRNet)) Intelink SharePoint pages. These sites are used for posting briefing slides, archiving past events, serving as a repository for cyber T&E resources (including the most recent policy and guidance), and linking to collaborative efforts. Figure 1-3 shows the unclassified landing page; the sub-pages are shown in the

[4] https://intelshare.intelink.gov/sites/te/CyberDT%20XSWG/_layouts/15/start.aspx#/SitePages/Home.aspx

[5] https://intelshare.intelink.sgov.gov/sites/cyberdt/XSWG/

left-hand column, and the links to collaborative efforts are along the top.[6] The unclassified page requires a Common Access Card (CAC) to access; the SIPR page requires SECRET clearance. IDA maintains both sets of pages.



Sub-pages are listed in the leftmost column; links to collaborative efforts are along the top.

Figure 1-3. Main unclassified Intelink SharePoint landing page of the CyberDT XSWG

G. Types of Activities

The two main recurring activities of the CyberDT XSWG are (1) large bi-annual in-person (or hybrid attendance) events, and (2) monthly virtual presentations.

The bi-annual events are three-day events held roughly twice a year. The topics/themes of these events are selected by the SSB. Hosting responsibilities rotate among the organizations represented by the SSB, and in-person and virtual attendance options are provided.[7] Typically, the first two days are a mix of briefings and breakout sessions held at both unclassified and classified (usually no higher than SECRET) levels. Time is built into the schedule for informal networking and for cyber T&E tool demonstrations. On the third day, referred to as "Mini Black Hat Day," Black Hat/DEF CON/Industry speakers are invited to give technical presentations. Continuing Education Unit (CEU) credits are given for attendance at Mini Black Hat Day.

The monthly virtual presentations are part of the CyberDT Cross-Service Informative Cyber Test Sync (Cyber DT XS InCyTS; pronounced "Insights") series. XS InCyTS started during COVID to maintain community engagement and have continued due to its

[6] C3D = Centralized Cyber Capabilities Directory; CRZ = Cyber Red Zone; CTCOI = Cyber Tools Community of Interest; OACRA = Ontology for Attacks in Cyber Risk Assessments; JCCOP = Joint Cyber Community of Practice; PWN2H0NE = DTE&A Bug Bounty.

[7] Hybrid attendance was first offered in July 2022 at CyberDT XSWG-14.

popularity. Topics and speakers for these monthly technical exchange meetings (TEMs) are solicited from the CyberDT XSWG membership and SSB.

2. History of Activities and Initiatives

As described in the previous chapter, the CyberDT XSWG hosts two main types of events and has spawned several initiatives, collaborations, and partnerships. The following sections describe each of these topics in detail.

A. History of Events

Figure 2-1 shows a timeline of all in-person/hybrid CyberDT XSWG events and virtual XS InCyTS events. Table 2-1 lists all of the in-person/hybrid events that the CyberDT XSWG has held, the host of each event, the location, dates, topic/theme, and number of attendees. Table 2-2 lists all of the virtual XS InCyTS events that the CyberDT XSWG has held, the host organization, title of the presentation, and number of attendees.

The average attendance at CyberDT XSWG events is 130 participants and the average attendance at XS InCyTS events is 100. At CyberDT XSWG-08, the decision was made to switch to semi-annual meetings from quarterly meetings. Virtual attendance was first offered in July 2020 with the start of the XS InCyTS series. As seen in Figure 2-1, there has been continued growth over the years with respect to attendance.

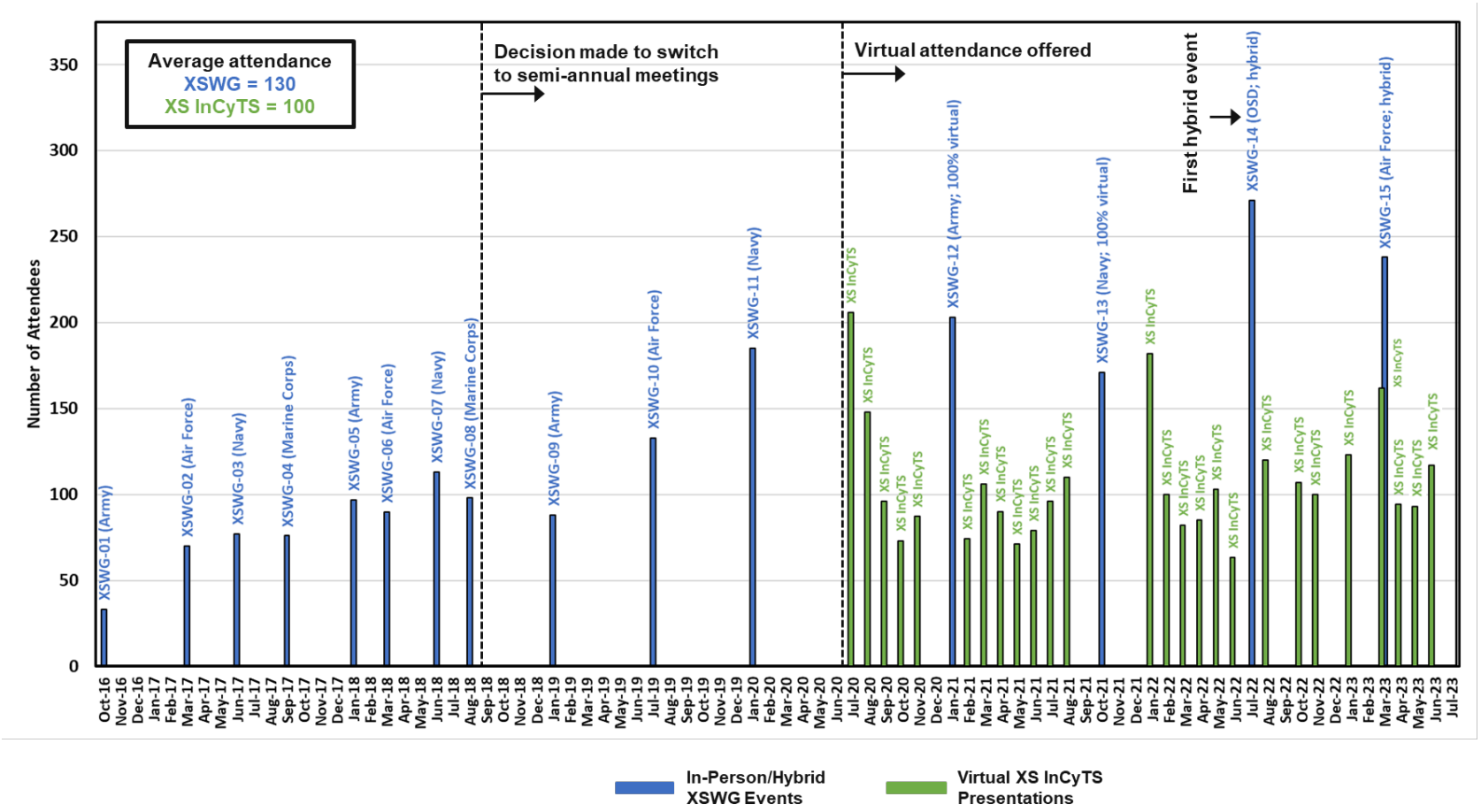


Figure 2-1. Timeline of events

Table 2-1. History of CyberDT XSWG In-Person/Hybrid Events

Event Name	Host	Location	Dates	Topics/Theme	Attendance
CyberDT XSWG-15	USAF 96th CTG	Eglin AFB / Niceville, FL and Virtual	7-9 Mar 2023	Cyber Test & Evaluation for Supply Chain	In-person: 149 Virtual: 89
CyberDT XSWG-14	IDA / DTE&A	IDA / Alexandria, VA and Virtual	12-14 Jul 2022	Challenges in Testing	In-person: 159 Virtual: 112
CyberDT XSWG-13	NCRC Charleston / NIWC Atlantic	Virtual	19-21 Oct 2021	What does Cyber T&E look like in FY22 and Beyond?	Day 1: 171 Day 2: 143 Day 3: 119
CyberDT XSWG-12	Army	Virtual	26-29 Jan 2021	Artificial Intelligence; Control Systems Cyber DT&E; Intelligence Support to Cyber DT&E	Day 1: 203 Day 2: 191 Day 3: 142 Day 4: 110
CyberDT XSWG-11	NSWC	Port Hueneme, CA	28-30 Jan 2020	Program Engagement; Workforce Education; Policy & Guidance Updates	185
CyberDT XSWG-10 and CTCOI	USAF 96th TW / 47th CTS	Eglin AFB / Niceville, FL	16-18 Jul 2019	Cyber Testing and Cyber Tools	133
CyberDT XSWG-09	Army RDECOM SLAD	Redstone Arsenal, AL	16-17 Jan 2019	Current Issues in Cyber Testing	88
CyberDT XSWG-08	USMC / ManTech	Stafford, VA	28-30 Aug 2018	Cyber Tools	98
CyberDT XSWG-07	NUWC	Newport, RI	26-28 Jun 2018	Fast Cruise, What is it?	113
CyberDT XSWG-06	Air Force	Joint Base Andrews, MD	20-22 Mar 2018	Cyber Intel; Cyber Initiatives	~90
CyberDT XSWG-05	Army ARL / SLAD	White Sands Missile Range, NM	30 Jan – 1 Feb 2018	Cybersecurity Testing Workforce	97
CyberDT XSWG-04	USMC	Quantico, VA	26-28 Sep 2017	No specific theme	76
CyberDT XSWG-03	NAVAIR	Pax River, MD	13-15 Jun 2017	SSB met and finalized the CyberDT XSWG Charter	77
CyberDT XSWG-02	Air Force	Joint Base Andrews, MD	28 Feb – 2 Mar 2017	Threats; NDAA 1647; Tools Infrastructure Governance	~70
CyberDT XSWG-01	Army	White Sands Missile Range, NM	25 Oct 2016	Who does Cyber DT across the Services and What are their Capabilities	33

Table 2-2. History of Virtual XS InCyTS Presentations

Date	Host	Title	Attendance
Jun 2023	Air Force	Using Advanced Framework for Simulation, Integration, and Modeling (AFSIM) to enhance MBCRAs and Cyber Testing	117
May 2023	Navy	Defense Research & Engineering Network (DREN) Overview	93
Apr 2023	DTE&A	Cyber T&E of AI Design Sprints	94
Mar 2023	Navy	Cyber Ready	162
Jan 2023	Army	Vulnerability Assessment Distributed Experimentation RedTeam (VADER) Range	123
Nov 2022	Navy	OneSAF-Cyber Assassin: Pilot Program to federate both simulations	100
Oct 2022	All Services	Cyber T&E for Supply Chain: Preparation for CyberDT XSWG-15	107
Aug 2022	Navy	AEGIS Virtual Twin	120
Jun 2022	TRMC	Distributed Cyber Infrastructure	63
May 2022	Air Force	Mission-based Risk Assessment Process for Cyber (MRAP-C) – Lessons Learned	103
Apr 2022	Navy	Demonstrated Cybersecurity Testing within the Navy, USS SECURE	85
Mar 2022	Army	Demonstrating Cyber Effects in a Distributed Cyber Environment	82
Feb 2022	Army	Joint Bold Quest	100
Jan 2022	NSA	Mission Critical Control System Cybersecurity	182
Aug 2021	DTE&A	CALDERA Phoenix-Networks Demo	110
Jul 2021	Air Force, TRMC	TDL (Tactical Data Link) Cybersecurity Projects	96
Jun 2021	SSB	La Jolla Logic – Advanced Tools for Cybersecurity & Anomaly Detection	79
May 2021	TRMC	TRMC T&E/S&T Cyberspace Test Technology – AI/ML projects	71
Apr 2021	JAIC	Joint Artificial Intelligence Center's (JAIC) efforts in T&E and challenges	90
Mar 2021	TRMC, Air Force	Cyber Test Tools Under Development	106
Feb 2021	Navy, NCRC	Cyber Red Zone	74
Nov 2020	All Services	Service Cyber T&E Workforce Efforts	87
Oct 2020	TRMC	TENA in Cyber featuring TENA Retina	73
Sep 2020	Army	Machine Learning Approaches to Validate Risk Assessment Findings	96
Aug 2020	Navy	Cyber T&E of Control Systems	148
Jul 2020	Air Force	Coordinating Intelligence Support to Cyber DT&E	206

B. Activities, Initiatives, Collaborations, and Partnerships

Section 4 of the CyberDT XSWG Charter states that in addition to bi-annual events, the WG will support other activities that "meet the needs of the community and … create change where possible." [2] Four such activities are described below; the Cyber Tools Community of Interest (CTCOI) and Centralized Cyber Capabilities Directory (C3D) are tool-related activities, and the Developmental Test Cyber Vulnerability Analysis (DT Cyber VA) standards and PWN2H0NE efforts are workforce-related.

1. Cyber Tools Community of Interest (CTCOI)

Cyber test tools have been a frequent topic of discussion within the CyberDT XSWG. In early 2017 at CyberDT XSWG-02, initial conversations were held about forming a group dedicated to tool development. Subsequent to that event, tools have been part of nearly every event agenda, either as a breakout session or as the overall theme of the event (see Table 2-1, as well as Table 2-2). The proposed tools-focused sub-group eventually became known as the Cyber Tools Community of Interest (CTCOI). In July 2019, CyberDT XSWG-10 was a joint CyberDT XSWG and CTCOI event. In March 2020, a Memorandum of Understanding (MOU) between the USAF 96th Cyber Test Group (CTG) and TRMC EA for Cyber Test Ranges was signed that formalized the activities of the CTCOI.[8] The CTCOI logo is shown in Figure 2-2.

Figure 2-2. The Cyber Tools Community of Interest (CTCOI) logo

The CTCOI currently uses an unclassified, CAC-enabled Intelink SharePoint page[9] as one means of communication with the cyber T&E community; a link to this CTCOI page can be found on the CyberDT XSWG page (see Figure 1-3). The CTCOI is a strong advocate for another CyberDT XSWG-spawned effort known as the C3D that is described below.

[8] The CTCOI is currently (July 2023) being reorganized and its processes are being updated.

[9] https://go.intelink.gov/tVjyWZ9

2. Centralized Cyber Capabilities Directory (C3D)

Among the tool-related discussions taking place during CyberDT XSWG-07 in June 2018, were conversations about the need for a resource that would help cyber T&E professionals identify and track current and future cyber T&E capabilities. In April 2019, DTE&A tasked an IDA team with identifying the necessary design, functionality, and requirements for a web-based "rolodex" of tools that was to be known as the Centralized Cyber Capabilities Directory (C3D). The C3D today is a CAC-enabled[10] searchable online[11] directory of cyber T&E tools, facilities, service providers, and people that is hosted by the Joint Federated Assurance Center (JFAC). [3] Its goal is to "promote cyber awareness and collaboration across DoD, the Services, and other organizations. Users can search for capabilities, connect with experts, and identify communities of practice for specific subject areas." [4] As of May 2023, over 900 user accounts have been created, and information on over 80 capabilities is available. [5] The C3D logo is shown in Figure 2-3. There is a link to the C3D on the CyberDT XSWG unclassified Intelink SharePoint page (see Figure 1-3).

Figure 2-3. The C3D logo

3. Developmental Test Cyber Vulnerability Analysis (DT Cyber VA) Standards

Beginning at CyberDT XSWG-05 in January/February 2018, the WG saw a need for establishing DT Cyber VA standards required for supporting and executing cyber DT activities. In November 2020, the WG developed and subsequently published a document that "assists DoD and industry Test and Evaluation (T&E) professionals with identifying developmental T&E cybersecurity knowledge, skills, and abilities (KSAs) that may be included in a qualification process or program for organizational-level and/or analyst-level qualification standards." [6]

[10] The C3D now also supports federal HSPD-12 credentials to allow access to non-DoD users such as those in the Department of Energy.

[11] https://jfac.navy.mil/c3d/

Standards were developed for both organizations and individuals. The DT Cyber VA Organization Qualification Standards address the following categories of Organizational Capability:

- O1-Professional Development;
- O2-Cyber VA Tools;
- O3-Laboratory and Facilities;
- O4-Human Capital;
- O5-Procurement;
- O6-Work Products Standards (Test Plan);
- O7-Work Product Standards (Final Report);
- O8-Legal Review Process;
- O9-Threat Intel Community Relationship;
- O10-Standard Operating Procedures.

The DT Cyber VA Analyst Standards include:

- 55 KSAs at the Apprentice Level;
- 65 KSAs at the Journeyman Level;
- 27 KSAs at the Master Level – Experienced Cybersecurity Analyst;
- 67 KSAs at the Master Level – Cyber T&E Lead Analyst.

The published DT Cyber VA Standards are available on the CyberDT XSWG unclassified Intelink SharePoint page.[12] Since their publication, the KSAs for Analysts have been used during the development of the annual Cyber Red Zone (CRZ)/Capture the Flag (CTF) training event.[13]

4. PWN2H0NE

Conversations about bug bounty events (i.e., crowd-sourced vulnerability discovery events) and the role they might play in DoD cyber T&E first started during the No-Host Social at CyberDT XSWG-10 in July 2019. The idea was formally proposed and explored

[12] https://go.intelink.gov/x01tFUU

[13] Cyber Red Zone (previously known as Capture the Flag) is an annual competitive training event designed by the Naval Air Warfare Center Training Systems Division (NAWC TSD) and hosted by the National Cyber Range. The event is designed to replicate the scenarios, equipment, and operational challenges that cyber teams from the Services encounter. NAWC TSD solicits input from the CyberDT XSWG SSB members regarding the attack types and training concepts to be included in each CRZ event.

in a breakout session at CyberDT XSWG-11 in January 2020. Based on interest and enthusiasm from the WG members, DTE&A funded an IDA study team to develop a framework for a DoD-tester-only bug bounty for systems in development. The IDA team also began outreach to potential partners, both programs who could offer a system to be the target, and testers who would be event participants. [7, 8, 9] The initiative was named PWN2H0NE (pronounced "pone to hone"), with "PWN" being cyber-speak for "being in control/dominating/owning", and "H0NE" having the dual meanings of "improving the system" and "improving the skills of the tester/participant" (hence the number "2" in the name). The event logo is shown in Figure 2-4. An event has not yet been executed and DTE&A is no longer leading/pursuing the PWN2H0NE effort[14], but will assist interested parties if requested.

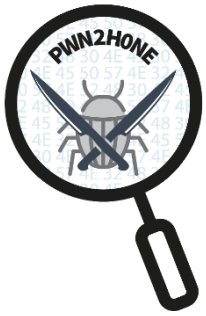


Figure 2-4. The PWN2H0NE logo

[14] Mr. Lee Kennedy, Dr. Kyle Morrison, and Dr. Noah Plymale, "PWN2H0NE: Summary of Activities, Observations, and Recommendations." IDA, 25 July 2023.

3. Member Feedback

The CyberDT XSWG has held 13 large in-person/hybrid and 2 large virtual events since October 2016. Post-event surveys have been distributed by IDA after most of these gatherings to collect feedback from the attendees about the event itself, and to understand more generally if the WG is meeting the needs of the members. The sections below discuss the results of those surveys. Note that surveys were either not distributed and/or the results are unavailable for CyberDT XSWG-01 through 06, 08, and 13[15].

A. Reasons for Attending

Post-event surveys for CyberDT XSWG-07, 09, 10, 11, 12, 14, and 15 asked attendees to indicate their primary reason for attending in-person/hybrid CyberDT XSWG events. As seen in Figure 3-1 and Figure 3-2, the two most frequently cited reasons are to **learn** and **network**.

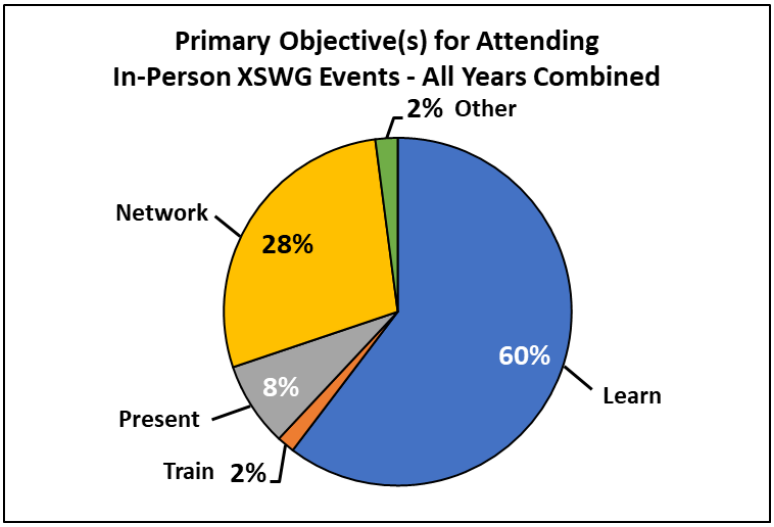
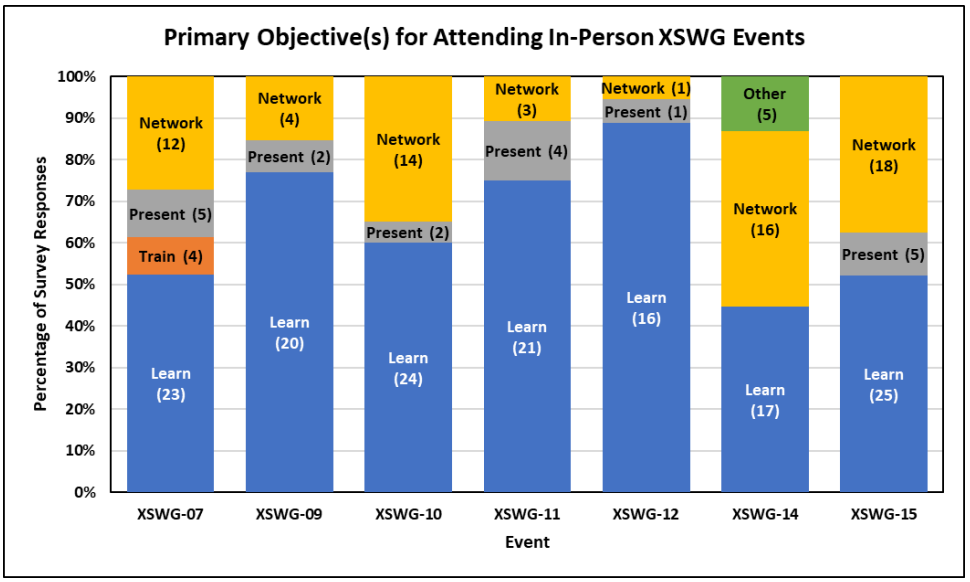


Figure 3-1. Primary Objective(s) for Attending In-Person CyberDT XSWG Events - All Years Combined

[15] Survey-related information for events 01-06 and 08 can unfortunately not be located due to a change in event facilitator leadership. An online survey was provided during event 13 due to a last minute switch from in-person to virtual format and only five participants provided feedback.



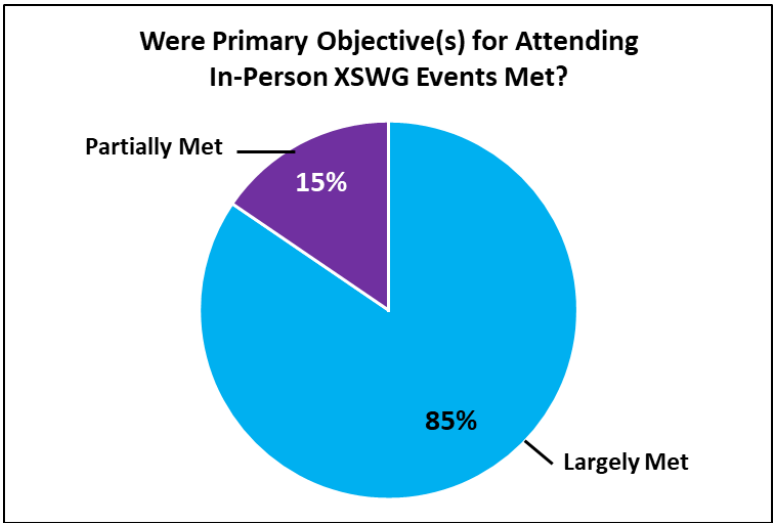
Values inside the parentheses indicate the number of responses per category.

Figure 3-2. Primary Objective(s) for Attending In-Person CyberDT XSWG Events – By Event

CyberDT XSWG-14, the first in-person/hybrid event offered after COVID, had the highest percentage of respondents indicating "Networking" as their primary objective compared with previous events; the importance of "Networking" was still high for CyberDT XSWG-15 attendees.

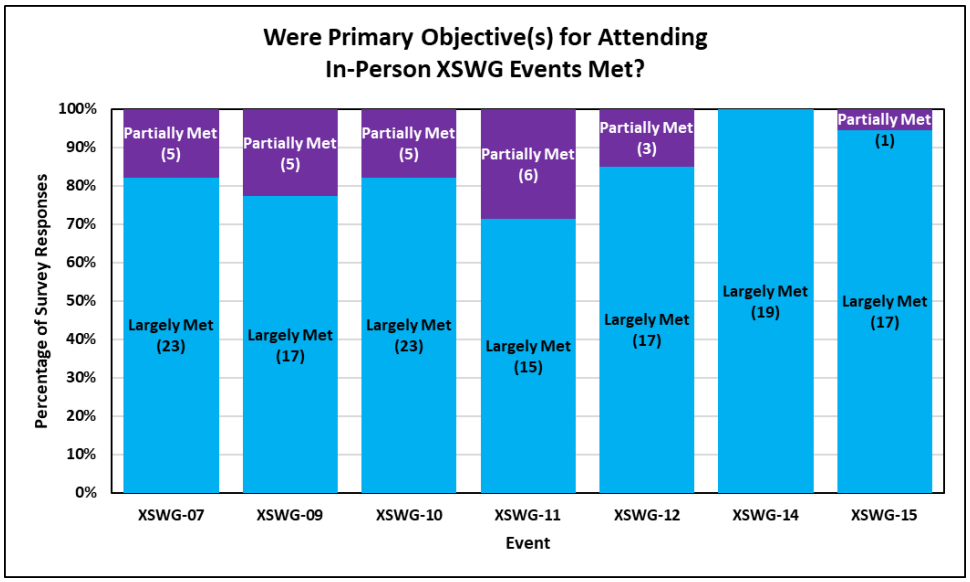
B. Satisfaction

The post-event surveys for CyberDT XSWG-07, 09, 10, 11, 12, 14, and 15 also asked attendees to indicate to what degree their primary reason for attending in-person/hybrid CyberDT XSWG events was met. Survey respondents overwhelmingly report that their objectives **were largely met**; no respondents chose the "Not Met" answer option. Figure 3-3 and Figure 3-4 show the breakdown of responses.



No survey respondents chose the "Not Met" answer option.

Figure 3-3. Were Primary Objective(s) for Attending In-Person CyberDT XSWG Events Met - All Years Combined



Values inside the parentheses indicate the number of responses per category. No survey respondents chose the "Not Met" answer option.

Figure 3-4. Were Primary Objective(s) for Attending In-Person CyberDT XSWG Events Met – By Event

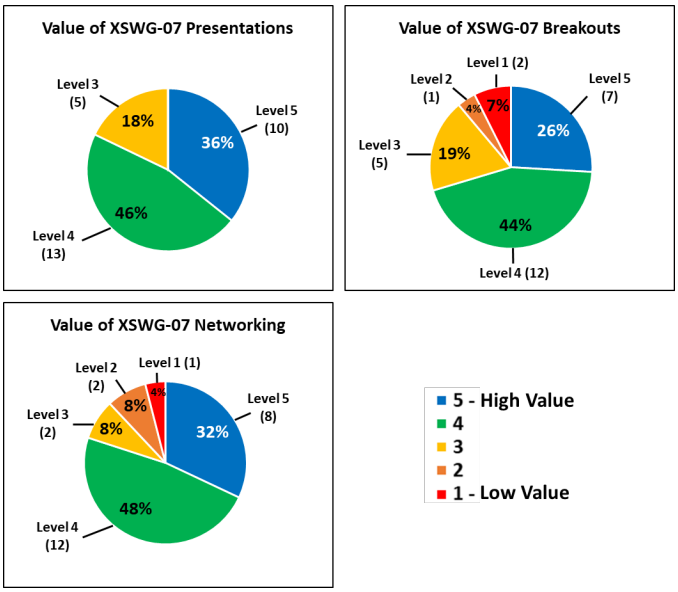
C. Value of XSWG Activities

As described earlier (see section 1.F), CyberDT XSWG events are a mix of activities including briefings, breakouts, tool demos, networking, and panels on Days 1 and 2, and mini Black Hat talks on Day 3. The following sections and figures present the responses collected from post-event surveys for CyberDT XSWG-07, 09, 10, 11, 12, 14, and 15 about how valuable the respondents considered each type of activity offered and attended to be.

1. Value of Main Event Activities

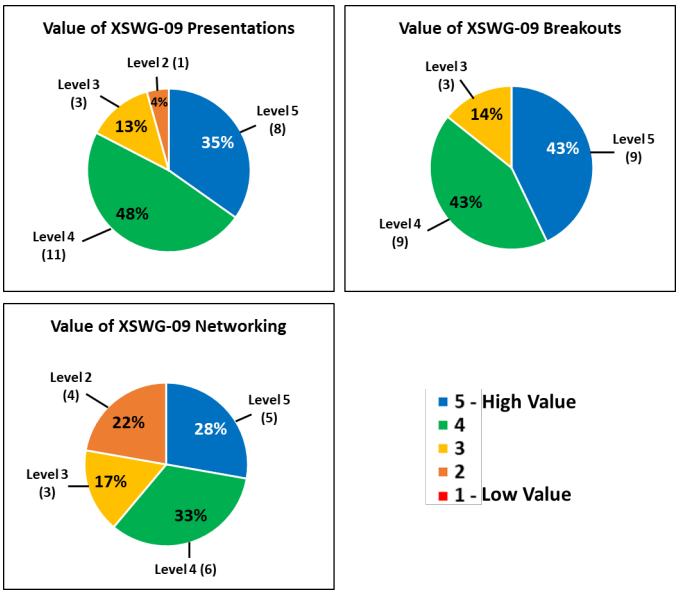
Post-event surveys for CyberDT XSWG-07 (Figure 3-5), 09 (Figure 3-6), 10 (Figure 3-7), 11 (Figure 3-8), and 12 (Figure 3-9) asked attendees to *rate the value* of each activity on a scale from 1 (low value) to 5 (high value). CyberDT XSWG-14 (Figure 3-10) and 15 (Figure 3-11) attendees were asked to *identify the most valuable* activity. Note that CyberDT XSWG-07, 09, 10, and 11 offered only in-person attendance, while CyberDT XSWG-12 was entirely virtual. CyberDT XSWG-14 and 15 offered both in-person and virtual attendance options.

With the exception of the Panel Session during CyberDT XSWG-11, more than 60 percent of survey respondents ranked **every activity offered** at CyberDT XSWG-07, 09, 10, 11, and 12 **at a value level of 4 or 5 (high value).** Only two activities at CyberDT XSWG-07 (breakouts and networking) and one at CyberDT XSWG-11 (networking) were reported to be of low value (level 1) by some attendees. The activity considered most valuable at CyberDT XSWG-14 was the Secret Briefings session; the Unclassified and Secret Briefings sessions were tied as most valuable at CyberDT XSWG-15. Based on these responses, **attendees find the main event activities to be valuable overall**.



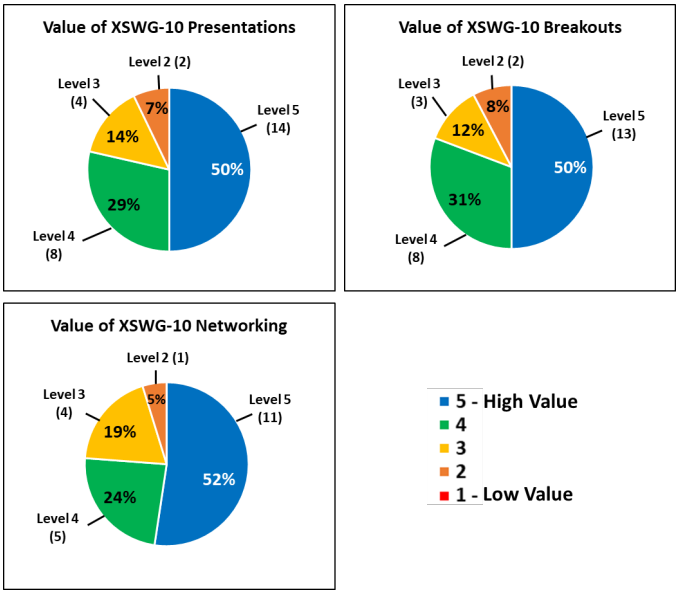
Values inside the parentheses indicate the number of responses per category.

Figure 3-5. Value of CyberDT XSWG-07 activities from post-event surveys



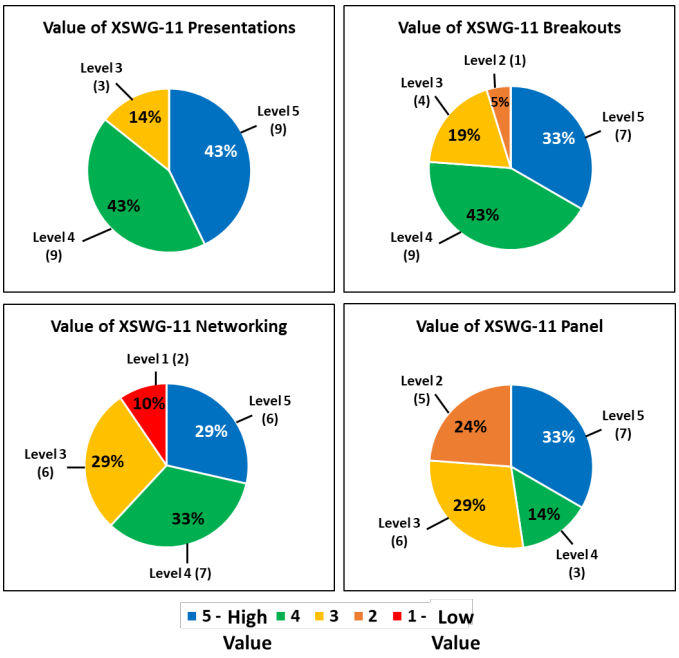
Values inside the parentheses indicate the number of responses per category.

Figure 3-6. Value of CyberDT XSWG-09 activities from post-event surveys



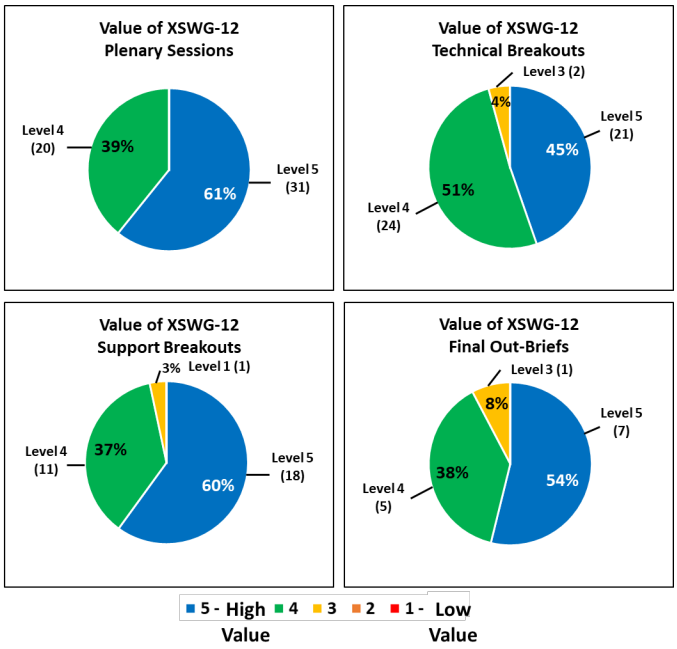
Values inside the parentheses indicate the number of responses per category.

Figure 3-7. Value of CyberDT XSWG-10 activities from post-event surveys



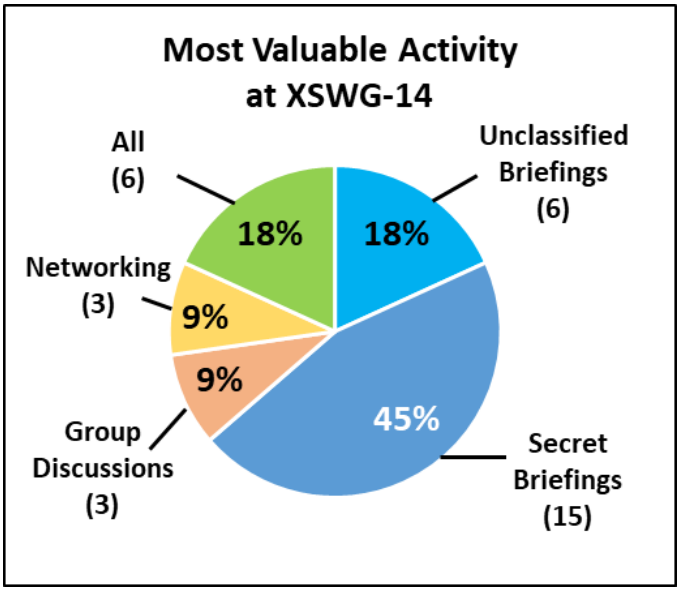
Values inside the parentheses indicate the number of responses per category.

Figure 3-8. Value of CyberDT XSWG-11 activities from post-event surveys



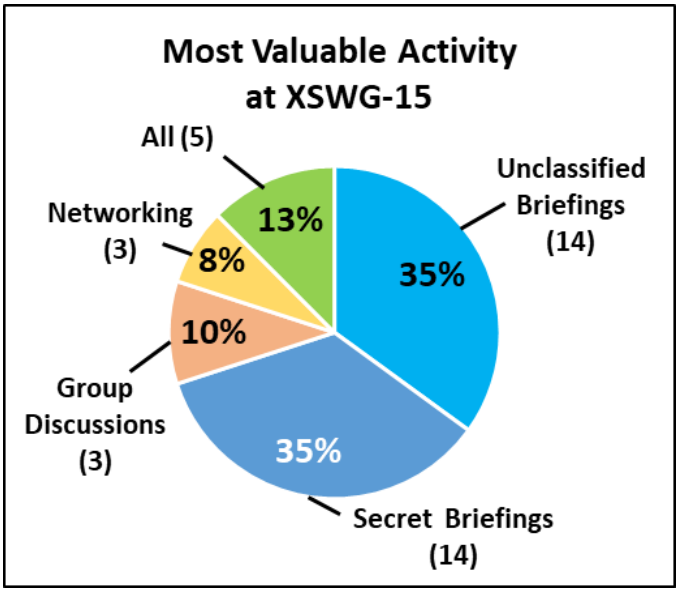
Values inside the parentheses indicate the number of responses per category.

Figure 3-9. Value of CyberDT XSWG-12 activities from post-event surveys



Values inside the parentheses indicate the number of responses per category.

Figure 3-10. Most valuable activity during Days 1 and 2 at CyberDT XSWG-14 from post-event surveys



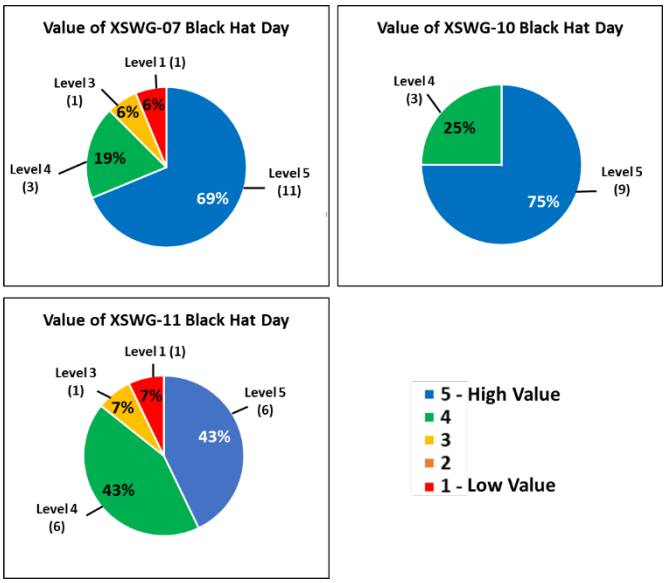
Values inside the parentheses indicate the number of responses per category.

Figure 3-11. Most valuable activity during Days 1 and 2 at CyberDT XSWG-15 from post-event surveys

2. Value of Mini Black Hat Day

Post-event surveys for CyberDT XSWG-07, 10, and 11 asked attendees to rate the value of Mini Black Hat Day on a scale from 1 (low value) to 5 (high value). Attendees at CyberDT XSWG-14 and 15 were asked to share their thoughts on Mini Black Hat Day.

As seen in Figure 3-12 and a representative selection of quotes, Mini Black Hat Day is considered to be a valuable activity by the majority of survey respondents, though some think the briefings can be too technical. Mini Black Hat Day provides the WG members with the opportunity to experience a portion of the large Las Vegas events without incurring the associated (large) costs (i.e., travel, time, and fees).



Values inside the parentheses indicate the number of responses per category.

Figure 3-12. Value of Mini Black Hat Day from post-event surveys

- **Representative selection of quotes from CyberDT XSWG-14 post-event surveys:**

  My group enjoyed the very technical deep dives, but felt that some of the content may have been too technical for some of the more senior leadership folks.

  Keep the mini black hat. Keep them technical.

  I greatly enjoyed mini black hat day. Listening to the hackers talk about how they approached a problem was fascinating. The only thing better would have been to watch in real time.

  Excellent training.

This section has always been a crowd pleaser, and is imperative to the event. It allows some of the "so what" to be seen, and for many folks who cannot get to a Black Hat in Vegas this is a fantastic preview.

Need less BlackHat tech stuff. Too specific for most attendees, including me!

- **Representative selection of quotes from CyberDT XSWG-15 post-event surveys:**

I think this is an amazing experience and helps to understand the outside of the DoD bubble and what the community is seeing. This is a must have for all future events.

Mini Black Hat often brings a non-DOD perspective that expands [the] thought process.

I thought the briefings were really interesting, but could not relate the material directly to my duties (working in weapons systems).

I was wanting to see real-time hacking capabilities and be able to [have] one-on-one discussions. The briefs were okay but somewhat diluted.

Really enjoyed the demonstrations and presenters.

D. Value of Overall CyberDT XSWG Effort

CyberDT XSWG-09, 10, 11, 12, 14 and 15 were asked to provide feedback on the value that the overall CyberDT XSWG effort had brought to them and their organization. As demonstrated by the representative selection of quotes below, the benefits reaped have been diverse.

Much greater awareness of efforts and issues in the community and several collaboration opportunities.

-CyberDT XSWG-09 attendee

Better perspective on DT.

-CyberDT XSWG-09 attendee

Knowledge of other available resources, methodologies.

-CyberDT XSWG-10 attendee

Huge networking value/opportunity to consolidate efforts/not repeat work.

-CyberDT XSWG-10 attendee

The knowledge that I received was very valuable due to the fact that I am a new hire.

-CyberDT XSWG-11 attendee

Better collaboration and info exchange between DT and OT activities.

-CyberDT XSWG-11 attendee

Opened my eyes in [sic] possible career paths and connections at my local base.

-CyberDT XSWG-11 attendee

Great information sharing and exchange.

-CyberDT XSWG-12 attendee

Better awareness of T&E community trends and topics.

-CyberDT XSWG-12 attendee

Understanding Who is doing What, Where and How; understanding Gaps/Lessons Learned; Networking with other efforts to Not Be Redundant or Duplicative with Critical Resources.

-CyberDT XSWG-14 attendee

The visibility into the thoughts and directions of the participating organizations is invaluable.

-CyberDT XSWG-14 attendee

The XSWG helps to engage communities and programs with new ideas and POCs that are available to help and make our overall security posture better.

-CyberDT XSWG-15 attendee

The primary value for me and my organization is in gaining a better and more complete understanding of the challenges and opportunities in the cyber T&E landscape.

-CyberDT XSWG-15 attendee

4. Senior Stakeholder Board (SSB) Self-Assessment

Current and former SSB members were asked in Spring 2023 to provide their written feedback regarding the value that the overall CyberDT XSWG effort has brought to their organization. They were also asked to identify the areas in which they feel the WG is meeting its stated goals and to provide suggestions for improvements in the areas where they feel the WG is falling short. The sections below summarize the feedback that was received.

A. Value of Overall CyberDT XSWG Effort

Echoing the feedback from the CyberDT XSWG membership via post-event surveys, the responding SSB members also think highly of the positive impact/influence that the WG has had on networking, information sharing, and improved communication.

> *"I think the biggest area where the XSWG has helped is it primarily provides a discussion venue for understanding the what and why cyber test is needed. The networking capabilities alone is a tremendous win. Program offices representatives are hearing directly from authoritive [sic] sources (R&E, DOT&E and cyber test agencies on what/when things should be done, what capabilities exist, how/who to connect to them. The [sic] is apparent to me during the early stages of an acquisition program where PMOs hear directly success stories on how early cyber involvement improved the product on delivery or transversely, how the lack of cyber hurt the program. There have been a number of programs who have heard the success stories at XSWG, come to us and say "That's what we want". Word of mouth here is powerful. Every meeting we have we get referrals."*

> *"We're a better, smarter, more engaged community because of the XSWG."*

> *"The XSWG has enabled us to extend our network throughout the joint cyber community. This has led to increased information sharing that spans methodologies to tools. Additionally, it has been instrumental in increasing our awareness and participation in Department level*

initiatives, policy, and guidance. Overall, I feel the XSWG is an incredibly valuable resource and one that should be continued and supported by all of the services."

B. Progress Toward Meeting WG Goals/Objectives

Feedback from the responding SSB members indicates that all six of the WG goals/objectives stated in the Charter, particularly the two "Promote" objectives, are being met. Though the responding SSB members did not indicate that any goals/objectives were entirely unmet, some members did report that they considered some goals/objectives to be only partially met. Overall, the responding SSB members report that the WG is productive and a worthwhile endeavor.

"I believe the XSWG is operating in the right space. I'm not aware of any other group/organization that has the membership, objectives, or activity level that is driving to promote jointness, policy, workforce, and technical excellence across the cyber community. The only add that may be of value is to charter sub working groups to address cyber community issues that can be promoted through policy, guidance, or best practices."

1. (Promote) Identify and disseminate lessons learned, results from internal research, and other subject matter expertise across the Test Teams.

a. Areas of Success

The responding SSB members report that this goal/objective is "clearly being met" by the XS InCyTS and CyberDT XSWG events. These SSB members consider the XS InCyTS TEMs to be a valuable addition to the line-up of activities provided by the WG. Additionally, they point to the continued growth of the WG that has led to difficulty in finding large enough venues to host in-person XSWG events as evidence of the value of these meetings.

b. Areas for Improvement

The responding SSB members did not identify any areas of improvement for this goal/objective.

2. (Promote) Identify opportunities for sharing of lessons learned and collaborative development of techniques, tools, CONOPs, analysis, metrics, reporting methodologies, and other best practices.

a. Areas of Success

The responding SSB members also report that this goal/objective is met by the XS InCyTS and CyberDT XSWG events. One member describes the XS InCyTS series as a "*tremendous success….[that] provides focused examples of techniques, tools and best practices*."

b. Areas for Improvement

The responding SSB members report that this objective would be more fully achieved if the WG were able to support classified discussions more frequently. Additionally, the formation of sub-working groups would help to maintain forward momentum in the areas identified in the goal/objective.

3. (Develop) Provide targeted training opportunities for Test Team personnel.

a. Areas of Success

Some responding SSB members report that this goal/objective is being met, with one offering Mini Black Hat Day at the CyberDT XSWG events as an example of such a training opportunity.

b. Areas for Improvement

The meaning of "training" was unclear to one responding SSB member, and another indicated that the training initiatives/objectives of Mini Black Hat Day should be more clearly articulated for each event. A recurring PWN2H0NE program supported by the National Cyber Range Complex (NCRC) was identified by another respondent as having the potential to be a beneficial training opportunity for the cyber T&E community.

4. (Develop) Provide an active and engaged forum for policy feedback and development; promulgate the latest policy and guidance to the Cyber DT&E professionals.

a. Areas of Success

The responding SSB members report that this goal/objective is being met, with one explaining that this is particularly the case when the WG has visibility into early draft products and the opportunity to provide feedback on those drafts.

b. Areas for Improvement

The responding SSB members report that an improved process for policy coordination would be beneficial.

5. (Enhance) Streamline the flow of current cyber intelligence information to Testers to assure timely application to system design.

a. Areas of Success

One responding SSB member reports this goal/objective as being met, but without elaboration.

b. Areas for Improvement

The responding SSB members indicate that there is room for improvement in this area, with one citing classification issues as one of the bigger obstacles preventing this goal/objective from being fully met.

6. (Enhance) Identify, implement, and develop measures of efficacy and efficiency related to Cyber DT&E implementation.

a. Areas of Success

One responding SSB member reports that processes that improve efficiency have been developed and implemented, but the same success with efficacy has not yet been achieved.

b. Areas for Improvement

One responding SSB member indicates that this goal/objective is mostly being met but is unsure "how the implementation of development of efficacy and efficiency are being measured or validated."

5. Overall Assessment of the CyberDT XSWG Effort

The CyberDT XSWG is a valuable resource for the cyber DT&E community that has made a lasting and continuing impact on its members and the DoD cyber DT&E enterprise. It is meeting many/most of the stated goals and objectives and activities listed in its charter, yet still has room to grow. Table 5-1 below summarizes the assessment of the WG; elaboration on the entries is provided in the subsequent text.

Table 5-1. Assessment of CyberDT XSWG Goals and Activities

WG Charter Sections 1 and 2: Purpose/Goals/Objectives	
• Promote	Met
• Develop	Partially Met; Room to Grow
• Enhance	Partially Met; Significant Room to Grow
WG Charter Section 4: Activities	
• Bi-annual meeting	Met
• Breakout sessions with products	Partially Met; Room to Grow
• Sub-working groups	Partially Met; Room to Grow
• Specialized training	Partially Met; Room to Grow
• Yearly goals	Not Met; Significant Room to Grow

A. Success in Meeting the CyberDT XSWG Mission

The stated mission of the CyberDT XSWG is to support and champion the needs of Service and Agency cyber DT&E professionals, specifically by promoting collaboration and knowledge sharing, developing best practices, and enhancing capability and influence. The group's charter outlines several activities that are intended to help achieve these goals.

1. Goal: Promote Collaboration and Knowledge Sharing

Recurring activities (i.e., the bi-annual XSWG events and the monthly XS InCyTS series) and sustained support of community-requested initiatives (e.g., CTCOI, C3D) aim to fulfill the goal of promoting collaboration and knowledge sharing. By many metrics, this goal is being met (see Chapter 2). The CyberDT XSWG has held 13 large in-person/hybrid events and 2 large virtual events since October 2016, as well as 26 virtual monthly TEMs since July 2020. Average attendance at these events is 130 and 100 participants, respectively, with attendance at the bi-annual XSWG events growing steadily over the

years. These events host unclassified and classified technical, policy, and workforce discussions, and the bi-annual XSWG events often include breakout sessions to dive deeper into topics of interest. Post-event surveys (see Chapter 3) have consistently shown that the WG members find these gatherings to be highly valued and a worthwhile investment of resources (i.e., time and/or travel). The learning and networking opportunities these events provide are cited as the core reasons for attending. The C3D and CTCOI are capabilities/resources initiated by the CyberDT XSWG to promote collaboration and knowledge sharing about cyber test tools and capabilities; both of these capabilities were initiated early on in the history of the WG (2017 and 2018, respectively) and are still on-going.

2. Goal: Develop Best Practices

Providing targeted training opportunities and contributing to the development of policy and guidance fall under the broad goal of developing best practices. Examples of ways in which the training/workforce goal is being met include (1) hosting speakers from Black Hat/DEF CON[16]/Industry during the bi-annual XSWG events, (2) developing DT Cyber VA standards, and (3) providing input to the design of the annual CRZ competitive training event. Mini Black Hat Day is a crowd favorite according to post-event surveys (see Chapter 3), and CRZ uses the DT Cyber VA Standards. The WG has hosted numerous briefings and breakout sessions at the bi-annual XSWG events and monthly XS InCyTS series on policy and guidance updates; these fora have provided opportunities for the cyber DT&E community to learn about the guidance that is in development and to give feedback regarding what they feel is working well and what needs improvement.

3. Goal: Enhance Capability and Influence

The "threat intel briefs" presented during the classified sessions of the bi-annual XSWG events are an effort to meet the goal of "streamlin[ing] the flow of current cyber intelligence information to Testers…". [2] (though there is still room for improvement in this area; see discussion in the next section). Many of the other briefings at the bi-annual and monthly events share the status and/or lessons learned from efforts to improve the efficiency of cyber DT&E.

4. Responsiveness to the Needs of the XSWG Membership

The WG has been responsive to the needs of its membership and has adapted and expanded its activities accordingly. The large XSWG events have switched from a quarterly to bi-annual cadence, and virtual attendance at these events is now also supported. The monthly virtual XS InCyTS series, originally started to maintain engagement during

[16] DEF CON is an annual hacker convention held in Las Vegas after Black Hat.

COVID, has continued and provides the WG with the opportunity to explore more topics and to discuss current events in a timely manner.

B. Areas for Improvement

There are opportunities for the WG to improve how it serves its membership; some changes will take more effort and creativity to implement, while others are relatively straightforward.

1. Identify Yearly Goals

The CyberDT XSWG charter states that the SSB will identify "Yearly Goals". [2] The SSB has not fulfilled this responsibility; no yearly goals have been generated since this activity was added to the charter in March 2020.

Generating a list of yearly goals would provide the CyberDT XSWG with a roadmap toward achieving the group's strategic goals. This would help to ensure that the activities, topics, and initiatives explored during the year have maximum impact.

We recommend that during the first SSB meeting of each fiscal year, the SSB decide on the yearly goals. Six months in, they should check the progress being made toward achieving each goal, and adjust as necessary. At the end of the fiscal year, the SSB should evaluate the overall success of the XSWG and identify areas for improvement.

2. Create Sub-Groups and Products

The CyberDT XSWG should facilitate the formation of sub-groups and/or support breakout sessions at the bi-annual events that generate "products" (e.g., white papers, guidance, processes, training materials). The formation of sub-groups and creation of products has not continued beyond the CTCOI and C3D.

These smaller, more focused groups have the potential to make an impact on current topics where knowledge in the cyber T&E community is still nascent (e.g., Artificial Intelligence and Autonomy), or areas where the community should improve communication and information flow with other organizations (e.g., cyber threat intelligence).

We recommend that the SSB consider alternating the format of the bi-annual events, with one event per year being "TEM"-style and the other being "working-group"-style. Additionally, the formation of sub-groups may be part of the conversation surrounding the identification of yearly goals.

3. Improve Ability to Hold Classified Discussions

The CyberDT XSWG should take steps to improve its ability to hold classified discussions, and have these discussions more frequently. Though a classified (SECRET) session is typically held during in-person XSWG events, the SSB currently does not think that the goal of sharing threat intelligence (e.g., improving awareness of processes and resources; improving communication between the intelligence and test communities) is being met.

Having the ability to discuss current efforts (e.g., application of tools, recent test events, identified vulnerabilities and mitigations) in a classified setting allows the group to discuss specifics and more fully appreciate the impact on cyber T&E. Being forced to speak about cyber threats in vague generalities dilutes the usefulness of that conversation.

We recommend that the SSB consider forming a sub-group tasked with identifying venues (in-person and virtual) accessible to the CyberDT XSWG that can support hosting these classified discussions, and to also identify speakers from the intelligence community who could provide a cyber threat intelligence briefing on a recurring basis. We also recommend that this sub-group explore the feasibility of holding these discussions more frequently (perhaps quarterly) rather than waiting until the bi-annual events.

4. Enhance Virtual Participation

The CyberDT XSWG should continue to facilitate, and further enhance, virtual participation. A 2021 IDA report found that supplemental funding for participants is needed to attend CyberDT XSWG events in person. [10] Post-event surveys also indicate an appreciation and desire for hybrid events:

> *The conference with both in-person and remote should be the norm. It will allow those who may not have time for the full conference to schedule time for topics that matter most to them.*
>
> *– CyberDT XSWG-14 attendee*

> *Virtual participation is not optimal, but it is the future. It expands the number of members who can attend.*
>
> *– CyberDT XSWG-14 attendee*

> *Liked the virtual format. Very likely I would not have been able to attend an in-person event even sans pandemic due to higher priority work, budget, etc.*
>
> *– CyberDT XSWG-12 attendee*

Supporting virtual attendance is important for making the XSWG as accessible to as many members as possible. It removes the requirement to secure travel funds and to attend

the entire event. Members can participate in sessions that are of the most interest to them and that fit within their busy work schedules.

Two ways of improving the virtual experience that are frequently suggested in post-event surveys are (1) better use of microphones, and (2) having a moderator who is dedicated to the virtual chat room. Ensuring that the microphones are high quality and working, and insisting that audience members hold their questions until they have a microphone to speak into, will help to make sure the virtual attendees can hear the discussion in the room and remain engaged. Similarly, having someone monitor the online chat room will improve the virtual attendees' participation by making sure their questions and comments are relayed to the in-person audience.

5. Improve Advertisement/Distribution of WG "Products"

The CyberDT XSWG should take steps to improve the advertisement/distribution of its "products." A 2021 IDA report found that most test organizations interviewed were unaware of the DT Cyber VA Standards that the CyberDT XSWG developed and published in 2020. [10] Similarly, a 2023 C3D User Survey conducted by IDA found that 86 percent of the survey respondents who indicated that they had never used the C3D (44 responses) said it was because they were unaware of the C3D; additionally, most respondents who *do* use the C3D (57 percent; 23 responses) were unaware of some of its recently added features. [5]

Though the XSWG roster is large and ~600 people regularly receive email announcements about its activities, that is only a small percentage of the ever-growing cyber T&E community. To enhance its impact and influence on cyber T&E writ large, the WG should publicize its efforts more broadly. The DT Cyber VA Standards can arguably be used by cyber T&E organizations and testers to improve funding, training, workforce retention initiatives, etc., *if* the community knows about them. Community engagement is critical for the C3D to survive and thrive. It is a resource built for and by the cyber T&E community; without their active participation, the information it holds will grow stale and eventually become outdated.

We recommend that advertisement and messaging become a topic of discussion at future XSWG events, and perhaps be a part of the SSB's yearly goals. Specific to the DT Cyber VA Standards, we recommend that the XSWG revisit these KSAs given the February 2023 issuance of DoDM 8140.03 "Cyberspace Workforce Qualification and Management Program". In an effort to increase the visibility of the C3D, announcements at the beginning of each monthly XS InCyTS presentation now include a list of the capabilities added to the directory since the last meeting and/or any new website features/functionality that have been released. We recommend that this practice continue and that the C3D team explore additional avenues for advertisement.

6. Increase SSB Visibility

The SSB members need to be more visible for it to be clear that the CyberDT XSWG is a Service-led initiative. The IDA support team frequently fields inquiries about who makes decisions for the CyberDT XSWG.

> *"I am curious, who is/are the 'Senior Stakeholder Board (SSB) Member' that approves the in-person registrations? Is that in my chain of command for mine? Or within the XSWG itself?"*
>
> *– CyberDT XSWG-15 attendee*

> *"Who are the representatives that make up the SSB?"*
>
> *– CyberDT XSWG-15 attendee*

It is important that XSWG members know who to reach out to when they have suggestions for driving change in the WG or across the cyber T&E enterprise. Visibility of the SSB will also improve accountability, promoting confidence among the membership that WG leadership will advocate for their needs.

The SSB has already taken one step toward improving its visibility during XSWG events: the SSB member associated with the Service hosting the monthly XS InCyTS event has begun facilitating the presentation (i.e., introducing the speaker, moderating questions, and making announcements about upcoming CyberDT XSWG activities). We also recommend that the SSB member associated with the Service hosting the bi-annual CyberDT XSWG events take a more visible leadership role during all stages of the planning (e.g., sending Save-the-Date and registration announcements, soliciting presentations, fielding questions about event logistics) and execution of the event. Additionally, we recommend that these events be held at a facility owned by the host Service.

7. Other Considerations

Below is a list of other considerations that will enhance/enrich the XSWG in the future if adequately addressed.

- It is vital that the SSB identify venues large enough to accommodate the increased in-person attendance and that can also support classified discussions. Once identified, these facilities should be reserved well in advance of future events.
- Verbal feedback from event attendees, outside of post-event surveys, has indicated that formal networking time at bi-annual events should be protected and increased. In order to support this request, the SSB should consider reducing the number and/or length of talks scheduled.

- Make the link between Mini Black Hat Day presentations and training objectives clearer.

(This page intentionally blank.)

6. Summary and Outlook

The CyberDT XSWG has been an active organization since its formation almost seven years ago. Motivated by the desire to bring together the cyber DT&E community to share knowledge and resources, the WG has grown in membership, expanded and spawned new activities, collaborations and partnerships, and been responsive to the needs of the community.

Overall, the CyberDT XSWG is meeting or partially meeting its stated mission and carries out nearly all activities listed in its charter. In particular, the WG excels at providing opportunities for learning and networking. Feedback from the members indicate that they have better visibility into many aspects of cyber T&E because of their participation in CyberDT XSWG events. They also appreciate the WG's continued support of virtual attendance post-COVID.

There is room for the CyberDT XSWG to grow in achieving its goal/objective of providing improved access to cyber intelligence. A small number of classified discussions are held at the bi-annual events and are only accessible to (appropriately cleared) in-person attendees. Identifying opportunities to increase the frequency of these discussions and exploring facilities that could support Secure Video Teleconference (SVTC) sessions would make a positive impact on the CyberDT XSWG. Equally beneficial would be the development of yearly goals by the SSB. The generation of a formal roadmap for achieving those goals would ensure that the group is well-positioned to address high-priority future T&E challenges. Finally, increasing the visibility of the SSB will elevate the voices of the WG membership as they will know who to contact with questions, suggestions, and concerns. Progress in these three areas would have the most impact on ensuring the continued success of the CyberDT XSWG in the future.

(This page intentionally blank.)

Appendix A. References

[1] M. A. Ambroso, A. E. Henninger, R. T. Merchand, K. A. Morrison and A. Vasilyeva, "D-8019 DoD Cybersecurity Test and Evaluation Capabilities and Gaps," Institute for Defense Analyses, Alexandria, VA, 2016.

[2] CyberDT Cross-Service Working Group, *Cybersecurity DT&E Cross-Service Working Group Charter V1.14,* 24 May 2023.

[3] P. J. Jaffke and R. Kuzio de Naray, "D-31865 Centralized Cyber Capabilities Directory (C3D) User's Guide v2.0," Institute for Defense Analyses, Alexandria, VA, 2021.

[4] P. J. Jaffke and E. F. Gauger, "Centralized Cyber Capabilities Directory," *DTE&A Newsletter,* no. 5, p. 5, 2023.

[5] E. F. Gauger, P. J. Jaffke and R. Kuzio de Naray, "D-33533 Analysis of the Centralized Cyber Capabilities Directory (C3D): Community Usage and Feedback," Institute for Defense Analyses, Alexandria, VA, 2023.

[6] Department of Defense, *Developmental Test Cyber Vulnerability Analysis Standards,* DoD Office of Prepublication and Security Review, Nov 10, 2020.

[7] R. Fischer, "A Sneak Preview of Cyber Buzz 8," *Cyber Resiliency Office For Weapon Systems Cyber Buzz,* no. 7, p. 12, 2021.

[8] C. R. Bucher, G. L. Kennedy and R. Kuzio de Naray, "Memorandum: Bug Bounty Program Framework for the Department of Defense (DoD) Test and Evaluation (T&E) Community," Institute for Defense Analyses, Alexandria, VA, 2020.

[9] L. Kennedy, K. Morrison and C. Bucher, "PWN2H0NE: Preparations Continue for the Initial DoD PWN2H0NE Event," *Cyber Resiliency Office for Weapon Systems Cyber Buzz,* no. 8, p. 4, 2022.

[10] C. Bucher and N. Plymale, "D-22746 Developments, Challenges, and Gaps in Cybersecurity Developmental Test and Evaluation: An Update on 2016 Findings," Instititute for Defense Analyses, Alexandria, VA, 2021.

(This page intentionally blank.)

Appendix B. Acronyms and Abbreviations

AF/TE	Air Force Test and Evaluation
AFMC	Air Force Materiel Command
AFOTEC	Air Force Operational Test and Evaluation Center
ARL	Army Research Lab
ATEC	Army Test and Evaluation Command
C3D	Centralized Cyber Capabilities Directory
CAC	Common Access Card
CEU	Continuing Education Units
CIO	DoD Chief Information Officer
COMOPTEVFOR/COTF	Navy Commander Operational Test and Evaluation Force
CONOPs	Concept of Operations
CRZ	Cyber Red Zone
CTCOI	Cyber Tools Community of Interest
CTF	Capture the Flag
CTG	Cyber Test Group

CTS	Cyber Test Squadron
CyberDT XSWG	Cybersecurity Developmental Test Cross-Service Working Group
DEVCOM DAC	Combat Capabilities Development Command Analysis Center
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DoD	Department of Defense
DOT&E	Director, Operational Test and Evaluation
DT Cyber VA	Developmental Test Cyber Vulnerability Analysis
DT&E	Developmental Test and Evaluation
DTE&A	Developmental Test, Evaluation, and Assessments
EA	Executive Agent
ED,DTE&A	Executive Director, Developmental Test, Evaluation, and Assessments
FFRDC	Federally Funded Research and Development Center
HSPD-12	Homeland Security Presidential Directive 12
IDA	Institute for Defense Analyses
JCCOP	Joint Cyber Community of Practice

JFAC	Joint Federated Assurance Center
JITC	Joint Interoperability Test Command
KSAs	Knowledge, Skills, and Abilities
MARCORSYSCOM	Marine Corps Systems Command
MCOTEA	Marine Corps Operational Test and Evaluation Activity
MCTSSA	Marine Corps Tactical Systems Support Activity
MDA	Missile Defense Agency
MOU	Memorandum of Understanding
NASIC	National Air and Space Intel Center
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Sea Systems Command
NAWC TSD	Naval Air Warfare Center Training Systems Division
NCRC	National Cyber Range Complex
NGIC	National Ground Intelligence Center
NIWC PAC	Naval Information Warfare Center Pacific
OACRA	Ontology for Attacks in Cyber Risk Assessments
ONI	Office of Naval Intelligence

OPNAV N94	Navy Test and Evaluation
OSD	Office of the Secretary of Defense
OTA	Operational Test Agency
OUSD R&E, DT&E	Office of the Under Secretary of Defense for Research & Engineering, Developmental Test and Evaluation
PWN2H0NE	DTE&A Bug Bounty “pone to hone”
SIPR	Secure Internet Protocol Router
SSB	Senior Stakeholder Board
STP&E	Strategic Technology Protection and Exploitation
SVTC	Secure Video Teleconference
T&E	Test and Evaluation
TEM	Technical Exchange Meeting
TRMC	Test Resource Management Center
TSMO	Army Threat Systems Management Office
UARC	University Affiliated Research Center
USA	United States Army
USAF	United States Air Force
USMC	United States Marine Corps

USN	United States Navy
USSF	United States Space Force
USSF/TE	United States Space Force Test and Evaluation
WG	Working Group
WSMR	White Sands Missile Range
XS InCyTS	Cross-Service Informative Cyber Test Sync

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
08-2023	Document	START DATE	END DATE

4. TITLE AND SUBTITLE
Assessment of the Cybersecurity Developmental Test Cross-Service Working Group and Recommendations for Improvement

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
HQ0034-19-D-0001		
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**
AX-1-3100		

6. AUTHOR(S)
de Naray, Rachel Kuz,io.; Savoy-Logan, Allison, J.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 730 East Glebe Road Alexandria, Virginia 22305	D-33585 H 2023-000260

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER
Ms. Sarah M. Standard Cybersecurity/Interoperability OUSD R&E, DTE&A		

12. DISTRIBUTION/AVAILABILITY STATEMENT
Cleared for Public Release by the DoD Office of Prepublication Review, Case 24-T-0072, 11 October 2023

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Cybersecurity Developmental Test Cross-Service Working Group (CyberDT XSWG) is a community that formed in 2016 to support and champion the needs of cyber test and evaluation (T&E) professionals. Its stated mission is to promote collaboration and knowledge sharing between Service and Agency cyber DT&E organizations, develop cyber DT&E best practices, and enhance cyber DT&E capability and influence within Defense Acquisition processes.

This document reviews the history of CyberDT XSWG activities and initiatives, post-event surveys completed by the WG members, and the results of a self-assessment conducted by CyberDT XSWG leadership, to evaluate the extent to which the CyberDT XSWG is meeting its objectives. Recommended actions that would improve the execution of the CyberDT XSWG mission are provided.

15. SUBJECT TERMS
developmental test; cybersecurity; working group; test and evaluation; collaboration and knowledge sharing

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	c. THIS PAGE		
Unclassified	Unclassified	Unclassified	SAR	

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER
Rachel Kuzio de Naray	703-933-6556