22nd ICCRTS

"Frontiers of C2"

Improving Cybersecurity Alignment and Integration

Paper 005

Topic 6: Interoperability/Integration and Security

Topic 2: C2 Concepts, Theory, Policy and Approaches

Topic 1: Operational Issues: Coalition Command and Control

Authors

Mr. Michael D. Tisdel

Mr. Ken D. Teske

Mr. Mark E. Miller

Mr. Patrick J. Guerin

Point of Contact

Michael D. Tisdel

Key Management Solutions

223 N Wahsatch Ave, STE 206

Colorado Springs, Colorado 80903-2253

(757) 203-5766 mtisdel@kmssecurity.com or michael.d.tisdel.ctr@mail.mil

Abstract

Cyber threats and attacks have an impact on any organization's ability to successfully conduct standalone operations or with organizational partners. Whether the operations conduct business administrative activities or command and control of military forces, cyber-attacks can have a disruptive effect on any organization's ability to operate. Each organizational partner has their own cyber strategy to address their cyber environment. To enhance operational success and reduce risk, organizational partners must use proven best practices and share cyber threat information with other organizational partner's. Alignment and integration of these strategies help address challenges of managing cyber defenses, the first step in alignment is to ensure your own network vulnerabilities are identified and actions are taken to ensure operations are not affected.

Applying the alignment framework, first introduced in the 19th International Command and Control Research and Technology Symposium, on an organization's network security efforts will help and ensure secure network operations for an organization. The first step in sharing Cyber information with partners is to have your network secured and proper processes and procedures established and effective. To accomplish this, using the alignment framework, we must look at the following four framework principles: Common vision, goals and objectives; Common understanding of the situation; Coordination of efforts; and Common measures of progress to change course if needed.

A secure network incorporates information assurance best practices, lessons learned, and the latest technology to address common network concerns. Using a framework methodology can directly improve network security for operations in the future.

Introduction

Practically all organization's in today's fast-paced, technology-driven world, ranging from private businesses, governmental departments or military organizations rely on information systems to get the right information to the right people at the right time to provide efficiency and effectiveness in decision making. Whether the decision deals with making daily administrative activities or conducting command and control of military forces, having the appropriate information available when needed allows for better decision making which will put you on the right path to organizational or mission success.

Unfortunately, there are adversaries throughout the world that want to intentionally or unintentionally disrupt your operations. Whether individual hackers attempt to penetrate a network for fun; cyber criminals attempt to extort money; or state-sponsored organizations attempt to conduct cyber espionage, there are adversaries that want to disrupt your organization's ability to operate with cyber-attacks.

> *"Cyber-Attack: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."* Source: NIST US Department of Commerce: Glossary of Key Information Security Terms, 2013

> *"Cyber-attacks can be as dangerous as conventional attacks. They can shut down important infrastructure. They can have a great negative impact on our operations… We are prepared for attacks that might happen in the future. Cyber-attack is something which is happening every day. And we are responding every day to different kinds of cyber-attacks."* NATO Secretary General Jens Stoltenberg said in November, 2014

> *"We must learn to negotiate a new geography, where borders are irrelevant and distances meaningless, where an enemy may be able to harm the vital systems we depend on without confronting our military power." US* President's Commission on Critical Infrastructure Protection, 1997

Since the 1990's cyber-attacks have been a constant threat for organizations and partners using networks to conduct operations. We have realized the need to share cyber information with other organizations and partners to help address security challenges with our networks and operations, whether it is denial-of-service attacks, data integrity issues or any other network and information threats. Successfully providing and sharing cyber-threat information and information assurance successes with other partners will help achieve collective goals for all.

Regardless of work or focus area, organizations are connected with other partner organizations worldwide via the internet. Each organizational partner has their own cyber strategy to address their own cyber environment. To enhance operation or mission success and reduce risk, each organizational partner must use proven network security and information assurance principles and share cyber threat information with other organizational partner's. For example, in the United States Government (USG) the Department of State, Department of Transportation, Department of

Defense, Department of Justice, etc., each have responsibility for their own cyber strategy but all are required to follow network security guidelines and information assurance guidance from the Department of Homeland Security which includes sharing of cyber threats with organizational partners. In that respect, note the parallels in the following information assurance definitions from various organizations and sources:

INFORMATION ASSURANCE Definitions:

US National Security Agency: The protection of information systems against unauthorized access to, or modification of, information, whether in storage, processing or transit, and protection against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. https://www.nsa.gov/about/faqs/terms-acronyms-faqs.shtml 2017

US Department of Defense: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Department of Defense Instruction 8500.01E, 2014

NATO Cooperative Cyber Defense Center of Excellence: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. https://ccdcoe.org/cyber-definitions.html 2017

Techopedia: Information Assurance (IA) refers to the steps involved in protecting information systems, like computer systems and networks. Steps include integrity, availability, authentication, confidentiality and nonrepudiation. https://www.techopedia.com/dictionary 2017

Figure 1. Information Assurance Definitions

Alignment and integration of these strategies help address the challenges of managing cyber defenses in support of all organizational partners. Considering the old adage, "You're only as strong as your weakest link," the first step in alignment is to ensure your own network security vulnerabilities are identified and actions are taken to include proper cyber protections and information assurance principles are applied to ensure organizational activities and operations are not affected.

This document describes the proposed use of the Alignment, Synchronization and Integration Framework (ASIF) which evolved from the Unity of Effort Framework that was first introduced in the 19th International Command and Control Research and Technology Symposium (ICCRTS), to address the issue of "Improving Cybersecurity Alignment and Integration." In general, each organizational partner has their own private, public, government, or military entity whose primary purpose is to develop strategies, guidance, and policies, which are to be implemented by network personnel, to address any cyber threats that affects the security of their network and data in their

public, government, or military areas. The intent of the strategies, guidance, and policies developed is to streamline and ensure secure network operations for their organizations.

As stated earlier, the first step in sharing Cyber information with partners is to have your own organization's network security and information assurance processes and procedures established and effective. To accomplish this, using the alignment framework, we must look at the following four framework principles in relation to your organization's information assurance efforts: Common vision, goals and objectives; Common understanding of the situation, "Common View"; Coordination of efforts; and, Common measures of progress to change course if needed.

In an ideal world, organizations worldwide, (whether private, public, governmental, or military) concerned with cyber threats and information assurance issues, would operate from an overarching collective strategic, operational and tactical plan to ensure alignment of information assurance efforts and secure networks. In fact, organizations face momentous obstacles ensuring that their plans and/or programs are based on shared assessments of conditions and appropriately aligned to develop, produce, and maintain a common view amongst organizational partners.

Problem

Per the US National Institute of Standards and Technology (NIST SP 800-150), Cyber threat information is any information related to a threat that might help an organization protect itself against a cyber threat or detect the activities of an actor.

NIST SP 800-150 also states that a cyber threat is "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service." In today's world it is inevitable, if connected to the internet, you will face a cyber threat. Thus, cybersecurity inoculation has to be a very high priority for any organization expecting successful operations.

> *"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards."* Gene Spafford, Professor of Computer Science, Purdue University, Computer Recreations: Of Worms, Viruses and Core War" by A. K. Dewdney in Scientific American, 1989

> *"If you spend more on coffee than IT Security, you will be hacked. What's more, you deserved to be hacked."* Richard Clarke, White House Cybersecurity Advisor, Cyber Conference, 2002

As stated in the information assurance definitions in Figure 1 above, information assurance involves intentional measures and actions taken to prevent unauthorized access, destruction, disclosure, or modification of information, and/or denial of service to an organizations operations and information systems. Proper network security and information assurance efforts not only

keeps your vital information out of unauthorized hands, but helps ensure that the information our decision makers need is available and reliable when they need it.

Most organizations understand that their networks are under constant threat from cyber-attacks. Most organizations (not necessarily all) on the internet have some sort of network security in place such as information assurance tools and processes which produce cyber threat information. They also know that the more cyber threat information they know, have, or receive, the better off they'll be in countering those threats.

The sharing of organizational cyber threat information is where the problem lies. Organizations don't necessarily share cyber threat information via their networks with other organizational partners for various reasons to include safeguarding proprietary, sensitive or classified information; or not having the capabilities, i.e., the necessary personnel, training, infrastructure, including tools and other reasons; *and the primary reason (we believe) is not having trust in other organizations having a secure network.*

Another problem in the "trust" area has to do with human factors.

> *"The weakest chain in cybersecurity is the human being. It's the lowest hanging fruit. Most of the attacks we see in the field right now are targeting uninformed people,"* Yves Lacombe, Technical Support Director at Vircom, 2017.

Each organization has a training program to teach or train it employees on the threats associated with Cybersecurity. An organization might have confidence in itself, but do they have confidence in the organization they are partners with. An effective training program in all organizations is essential to reduce the human factor impact of trust between organizations.

To enhance operation or mission success and reduce risk for all, organizational partners must better understand the benefits of information sharing; use of proven information assurance principles; and take the necessary actions to share cyber threat information with other organizational partner's. Successfully providing and sharing cyber threat information and information assurance successes with other partners will help achieve collective goals for all.

Using the ASIF is one way of accomplishing this function.

Background

In the summer of 2014, this team proposed a solution and repeatable processes to improve Unity of Effort at the 19th ICCRTS in a paper titled "Methodology to Improving Unity of Effort for Mission Partner Planning" [Ref. A]. The Unity of Effort framework, (of which the Alignment, Synchronization, and Integration Framework (ASIF) later evolved) was developed as a multi-purpose planning aid to facilitate USG stakeholders' coordination, synchronization, visibility and information sharing for improving unity of effort. The framework helps to identify gaps, seams, and redundancies amongst stakeholders, and helps focus similar efforts to achieve national goals

and objectives. The Unity of Effort framework is now an established "Best Practice" for DOD and others.

The US Combatant Commands needed a consistent and institutionalized approach to plan and resource military support for Civilian Agencies and improve unity of effort toward meeting national and strategic objectives at the operational/theater campaign level. The goal was to achieve broad consensus on the approach to work towards common objectives, applied across different geographic regions by all elements of national and international power acting in concert.

> *"One of the explicit lessons of the last decade of conflict is the absolute necessity to share information, plan, and operate in concert with our interagency and foreign partners."* Admiral McRaven, Commander, USSOCOM, 2011

All Government organizations concerned with national security should operate from an overarching joint strategic plan at the global, regional, and country-level to ensure alignment of various government efforts. This would then be aligned with other governments who in all reality face the same significant hurdles to ensure their plans and/or programs are based on shared assessments of conditions, are appropriately aligned, and account for each other's capabilities, capacities, and activities.

Within each organization, differences in organizational priorities result in critical differences at the department and organizational level that effect theater and regional planning. The differences were viewed in this effort as inhibitors to unity of effort. We will discuss these in greater depth later in this paper.

The most important difference between the Unity of Effort framework and other approaches to USG planning was that each organization could continue to operate using their own planning and programming processes while mapping to a common Unity of Effort framework. To apply the Unity of Effort framework, stakeholders must meet, communicate, and collaborate to gain consensus of a common view and common understanding of the situation. These "consensus" gathering meetings, by their very nature, improve unity of effort and may be the most important part of this process.

The foremost goal of the Unity of Effort framework was to create a common understanding of who is doing what, where, and when in the area of importance to work together to improve unity of effort towards meeting agreed upon goals and objectives.

As mentioned earlier, in 2014, stakeholders at the time collectively identified over twenty reasons, rationales, and explanations, which impede unity of effort. We call these reasons, rationales, and explanations "*inhibitors*". Today, we find that there are no major changes to stakeholder beliefs on these inhibitors. Below in Table 1, as identified by stakeholders, are the top twelve inhibitors to unity of effort.

If the twelve inhibitors identified below (based on past research and continuous monitoring) degrade alignment and synchronization, and by extension, planning, then it would be a logical assumption that the mitigation of one (or more) of those inhibitors would thereby improve planning and alignment. To keep stakeholders in the sphere of reality, it must be pointed out that there are certain "inhibitors" that by their very nature seem impervious to any mitigation attempts to address the inhibitor. However, this does not preclude attempts to solve these issues and offers the opportunity for further examination in decomposition.

Top Twelve Inhibitors to Unity of Effort	
1. Stovepipes/silos (lack of information sharing)	7. No established process (ad hoc)
2. No visibility of efforts and activities	8. No global repository of information
3. Partner nations confused over mixed messages	9. No forcing function to drive unity of effort
4. Lack of planning resources	10. Conflicts in planning timelines
5. Differing lexicon/taxonomy/language	11. Uncoordinated efforts
6. Disparate activities	12. Competing priorities

Table 1. Inhibitors to Unity of Effort

Alignment, Synchronization, and Integration Framework

This conceptual approach to building an ASIF is a way to visualize components of existing plans, programs, and activities to improve the distribution and application of scarce resources with maximum positive effect. The structure, definitions, templates, and how-to instructions of the ASIF are repeatable and reusable for any subject area or mission set. However, each application of the Framework will produce unique products for each stakeholder, mission set, and operating environment. The Framework consists of a how-to guide (the Solution Guide), along with a set of templates for "Stage 1" the initiation phase, "Stage 2" the three-dimensional view, "Stage 3" the matrix view, and "Stage 4" what we call the deep dive or detailed stage of planning as shown in Figure 2 below.

Stage 1 of the framework is initiated by normal planning or directed by higher-level guidance. It also consists of identification of stakeholders and mission partners that have an investment, share, interest or desire to address the stated issue or problem set.

Stage 2 is achieved by stakeholders and mission partners identifying and coming to consensus on common objectives, common operating environments and common categories of effort and a common lexicon that all stakeholders can work with.

Stage 3 is a view of stage 1 and 2 information displayed in a matrix where stakeholders can identify key focus areas called key intersections. Stage 3 also identifies whether a stakeholder is the lead or a contributor for a mission area or issue determined by law, directive, and precedent. A stage 3 view is presented later in the paper.

Stage 4 is an optional phase of the framework. It is useful when stakeholders need or desire additional work to identify capability or capacity gaps, coordinate activities, and or develop specific recommendations to address inhibitors or impediments to unity of effort.

The Framework is a viable repeatable process for improving planning. Repeatable in this context, a repeatable process refers to processes, procedures, workflows, and templates that are reusable framework components. Repeatable processes allow a team to make efficient use of framework mechanisms that have proved to be successful in the past and reduce unnecessary variations that can take up time, effort and resources.

In each of the stages analysis is conducted on the issues of the stage. In the first two stages of the Framework; identifying stakeholders, having them develop (and reach consensus on) common objectives, and explaining their operating environment removes and/or mitigates four out of the top twelve inhibitors (differing lexicon, no visibility, no established process, competing priorities). These inhibitors were identified in Table 1 and, will be discussed later. Below is a graphic view (Figure 2) for building the quick reference guide and attributes for each stage of the original Unity of Effort Framework to aid in understanding of the process [Ref. C].

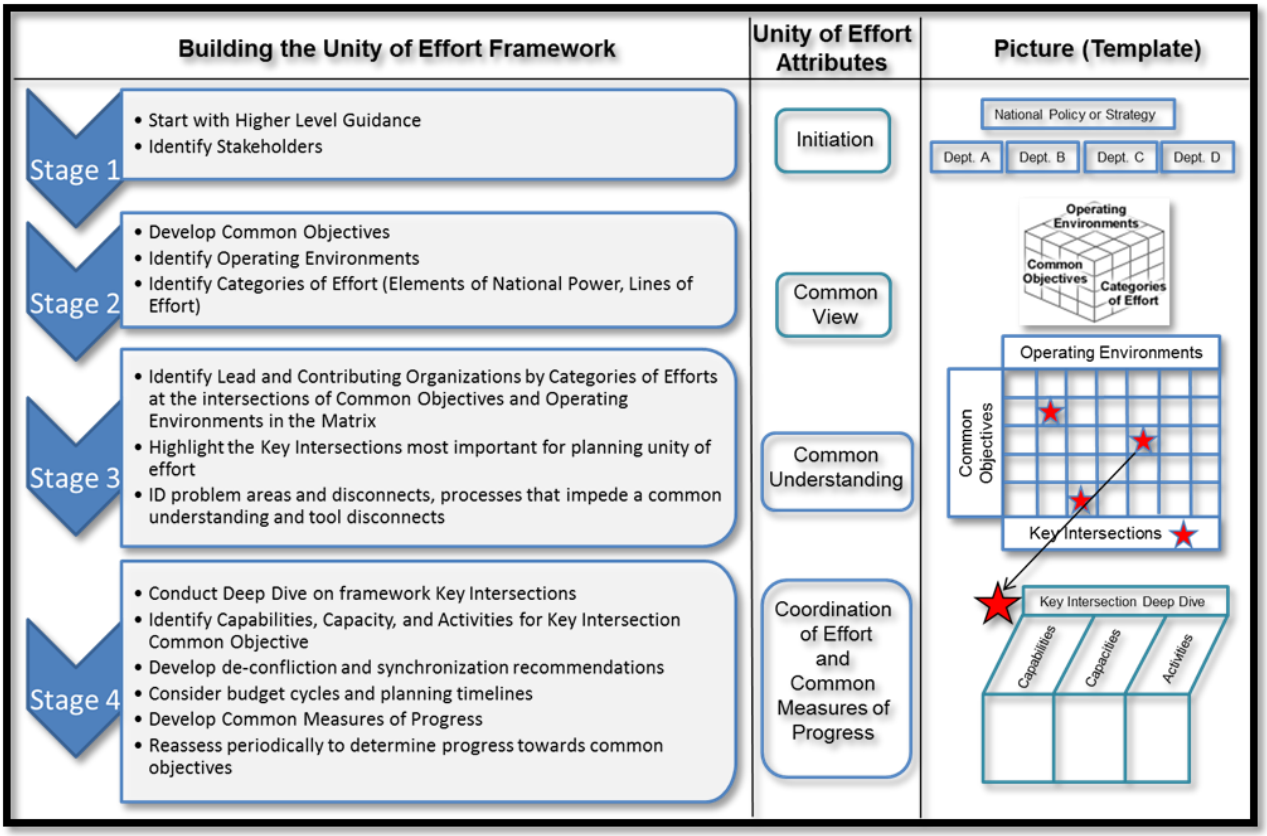

Figure 2. Original Unity of Effort Framework

Alignment, Synchronization, and Integration Application

Through our work supporting an organization in Europe we were asked to review the status of the unit's network(s). In this process we reviewed network documentation, vulnerabilities, and security. It was identified that network(s) documentation and understanding of authorities to operate a network were lacking; IA Requirements, policy, and guidance was limited; and no intrusion detection system (IDS) was installed on the network (opening the network up to cyber threats). Accepted standard best practices state that as a minimum an IDS are required to monitor and detect malicious activity on the network. A purpose-built device or tool to monitor the network for malicious activity is ultimately required to meet government and industry best practices.

That being said, to help this organization with securing their network and eventually their ability to share cyber threat information with organizational partners, we proposed using the ASIF to address network security, understanding of the network, and information assurance issues to ensure the organization had their network in order.

To address these challenges our team started with the baseline of the ASIF (an evolution of the Unity of Effort framework), commonly known as the "Dashboard" [Ref. C] and seen in Figure 3 below.

To begin our process, we conducted stage one of the ASIF to identify any overarching guidance documents and authoritative directives applicable to the problem set. After identification of applicable documents, we researched and reviewed US DOD and North Atlantic Treaty Organization's (NATO) guidance documents covering Cyber, network security and information assurance. From that research, we identified the key stakeholders involved with the issue in the unit and outside of the unit. We then created a contact list and started a list of consensus key terms and definitions.

As a review, stage two of the ASIF consists of identifying common objectives, operating environments, and categories of effort. In this analysis and use of the ASIF, as the framework is extremely adaptable, we modified stage two to focus on network areas of interest, network issues and vulnerabilities, and network issue involvement (who in the unit is involved with network issues). The modifications of the framework are displayed in figure 4 below, as the dashboard for the project addressing the efforts to secure the network. You will notice that the new dashboard only has the first three stages as it was decided to not venture into stage 4.

The network areas of interest analysis identified the following areas: Communications Security, Network (Unclassified and classified level), Software, Hardware, Data Center (information Integrity), Mobile Environment, Virtual Desktop Infrastructure (VDI), Remote Access System (RAS), Information Assurance (availability, integrity, authentication, confidentiality, non-repudiation), Configuration Management, Enterprise Architecture, Network Continuity of Operations (COOP) (emergency response, backup operations, post disaster recovery), malicious user and Federated Connection.

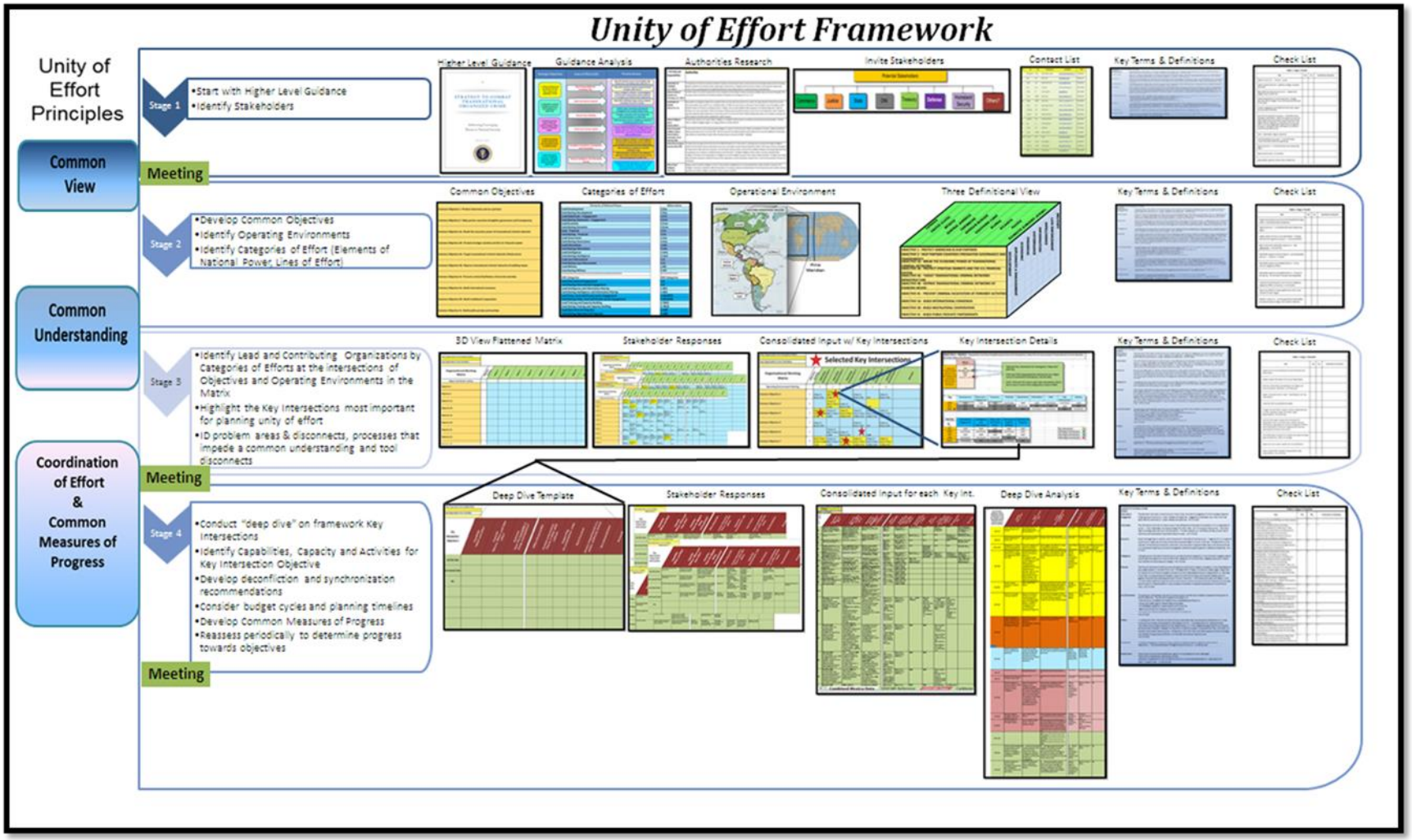

Figure 3. Original Unity of Effort Framework Dashboard

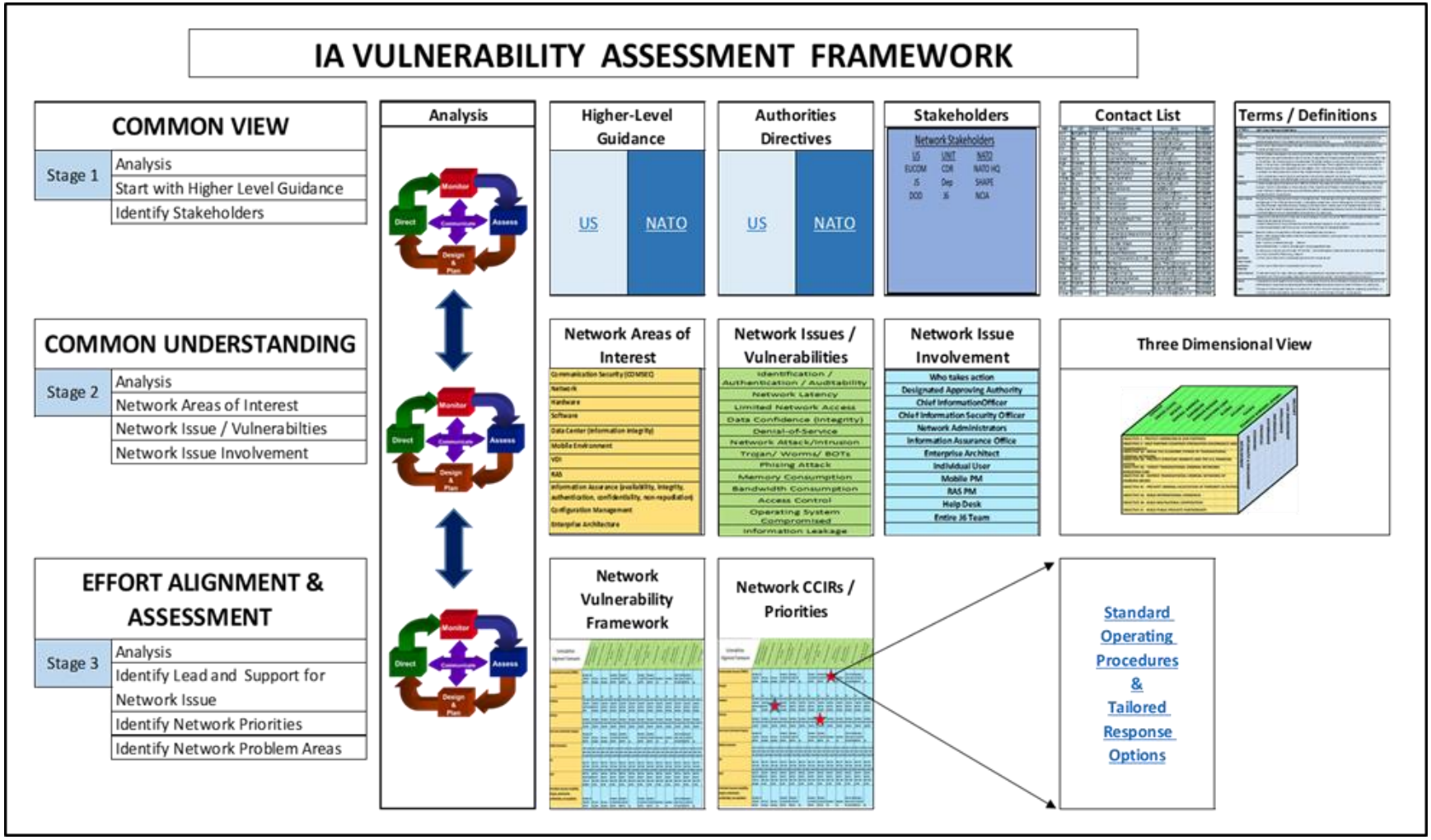

Figure 4. IA Vulnerability Assessment Dashboard

The consensus network issues and vulnerabilities analysis identified consisted of the following areas: Identification /Authentication/ Auditability, Network Latency, Limited Network Access, Data, Confidence (integrity), Denial-of-Service, Network Attack / Intrusion, Trojan /Worms / BOTs (web robots), Phishing Attack, Memory Consumption, Bandwidth Consumption, Access Control, Operating System Compromised, and Information Leakage.

The consensus network issue involvement (personnel involved with network operations) the team identified consisted of the following: Designated Approving Authority, Chief Information Officer, Chief Information Security Office, Network Administrators, Information Assurance Office, Enterprise Architect, Individual User, Mobile Program Manager, RAS Program Manager, Help Team and the entire J6 Team.

The development of the network areas of interest, the network vulnerabilities and issues, and the identification of personnel involved in the network helped develop and support the stakeholder's transition from stage 1 common view to their common understanding of network issues in stage 2. This common view and understanding led to the identification of gaps in network security and documentation in stage 3.

As mentioned before, in stage 3 the stakeholders are able to view stage 1 and 2 information in a matrix that allows further analysis of the network issues. This is displayed in the IA Vulnerability Assessment Matrix displayed in Figure 5 above.

After the identification of gaps in stage 3, we are able to identify network problem areas and then assign network priorities to those problem areas. The identification of who should be involved in the various network issues and priorities helped align work efforts in the unit. From the authoritative sources identified earlier in Stage 1 of the ASIF process, duties and responsibilities are assigned for each of the people identified who have network involvement. This is displayed in Figure 5 above. By applying and using government and commercial best practices for network security and information assurance, the unit will be able to build and establish standard response plans and tailored response options to any network issue that might arise from cyber threats identified in the network issues and vulnerabilities in the areas identified in the network areas of interest.

Implementing both government and commercial best practices, along with and implementing and using the standard operating procedures and tailored response options, (to include an intrusion detection system), would provide a means to determine and assess common measures of progress and provide for greater understanding of capability sets.

Vulnerabilities Alignment Framework	Identification / Authentication / Auditability	Network Latency	Limited Network Access	Data Confidence (Integrity)	Denial-of-Service	Network Attack/Intrusion	Trojan/ Worms/ BOTs	Phising Attack	Memory Consumption	Bandwidth Consumption	Access Control	Operating System Compromised	Information Leakage	Comments
Communication Security (COMSEC)	Net Admin / IA / Mob PM / NCEP PM	HD / User / Net Admin	HD / User / Net Admin	Net Admin / IA / Mob PM / NCEP PM	Net Admin / IA / Mob PM / NCEP PM	ALL	Net Admin / IA / Mob PM / NCEP PM	Net Admin / IA / Mob PM / NCEP PM	Net Admin / CIO	Net Admin / CIO	CISO / IA / Net Admin / Mob PM / NCEP PM	Net Admin / IA / Mob PM / NCEP PM	ALL	
Network	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	
Hardware	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	CIO / CISO / IA / Mob PM / RAS PM / Net Admin	
Software	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	Net Admin / IA / Mob PM / RAS PM / HD / User	
Data Center (Information Integrity)	Net Admin / IA / Mob PM / RAS PM / User / CISO	HD / User / Net Admin	HD / User / Net Admin	Net Admin / IA / Mob PM / RAS PM / User / CISO	Net Admin / IA / Mob PM / RAS PM / User / CISO	ALL	Net Admin / IA / Mob PM / RAS PM / User / CISO	Net Admin / IA / Mob PM / RAS PM / User / CISO	Net Admin / CIO	Net Admin / CIO	Net Admin / IA / Mob PM / RAS PM / User / CISO	Net Admin / IA / Mob PM / RAS PM / User / CISO	ALL	
Mobile Environment	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	
VDI	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	DAA / CIO / CISO / Net Admin / Mob PM / RAS PM	
RAS	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	RAS PM / Mob PM / CISO / IA / Net Admin / DAA	
Information Assurance (availability, integrity, authentication, confidentiality, non-repudiation)	Net Admin / RAS PM / Mob PM / User	HD / User / Net Admin	HD / User / Net Admin	Net Admin / RAS PM / Mob PM / User	Net Admin / RAS PM / Mob PM / User	ALL	Net Admin / RAS PM / Mob PM / User	Net Admin / RAS PM / Mob PM / User	Net Admin / CIO	Net Admin / CIO	CISO / IA / Net Admin / Mob PM / RAS PM	CIO / CISO / Net Admin / IA / Mob PM / User / RAS PM	ALL	
Configuration Management	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	DAA / CIO / CISO / Mob PM / NCEP PM	
Enterprise Architecture														
Network Contingency COOP (emergency response, backup operations, post disaster recovery)	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	
Malicious user	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	DAA / CIO / CISO / IA	
Federated Connection	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	CISO / Net Admin / IA / Mob PM / RAS PM	

Figure 5. IA Vulnerability Assessment Matrix

Alignment, Synchronization, and Integration Analysis

Our Analysis (Table 2 below): Through discussion and feedback with unit members in various sections of the organization, (to include members that were responsible for maintaining the network, members of the unit that just used the network, and leadership that was responsible for the network), it was evident that "Significant Improvement" in a Common View, Common Understanding and increased Alignment of Efforts would result in implementation of the Information Assurance Vulnerability Assessment framework. The results, which are summarized in Table 2, were based on three factors: stakeholder agreement, increased visibility, and capability awareness significance.

Unity of Effort Attribute	Evaluation metric	Initial Baseline	Final Result
Common View	Does the Alignment, Synchronization and Integration Framework application mitigate the occurrences of mixed or confusing messages about network security and information assurance?	Possibly	Conclusively
Common Understanding	Does this Alignment, Synchronization, and Integration Framework application provide for common lexicon and terminology understanding?	Conclusively	Conclusively
Alignment of Efforts	Does this Alignment, Synchronization, and Integration Framework application identify areas to focus resources?	Possibly	Conclusively
	Does Alignment, Synchronization, and Integration Framework application improve the ability to align efforts with mission partners?	Possibly	Conclusively
Common Measures of Progress	Does this Alignment, Synchronization, and Integration Framework application provide the means to determine common measures of progress and provide for greater understanding of network vulnerabilities and information assurance	Possibly	Conclusively
Usability	Does this Alignment, Synchronization, and Integration Framework application provide useful capability to organization?	Inconclusive	Conclusively

Table 2. "Significant Improvement"

Conclusion

The Alignment, Synchronization, and Integration Framework is based on four principles:

1. Common vision, goals, and objectives for the mission;

2. Common understanding of the situation;

3. Alignment of efforts to ensure continued coherency; and

4. Common measures of progress and ability to change course as needed

The ASIF, in this instance, improves understanding and alignment to address network security challenges and makes contribution to many other issues which rely on network operations. It also allows the unit to be able to share cyber threat information with organizational partners as trust is established via implementing and using government and commercial best practices.

> "Such a comprehensive alignment management concept uniquely recognizes that any organization, department, or even program, even if it has its own mission, vision, strategies, and critical success factors, is only one element of a larger delivery and service mechanism. In nearly all cases the success of strategy to execution depends on the ability to operate in alignment and therefore unity with the rest of the organizations with a common stake in the issues" [Ref. E].

The result of having a network properly secured is the opportunity to get the right information to the right people at the right time to provide efficiency and effectiveness in decision making. Whether the decision deals with making daily administrative activities, correcting network issues, or conducting command and control of military forces, having the appropriate information available when needed allows for better decision making which will put an organization on the right path to organizational or mission success.

Appendix A: Glossary

Access Control: Access control a is way of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information. Techopedia.

Alignment, Synchronization, and Integration Framework: Unity of Effort Framework renamed.

Authentication: A process that ensures and confirms a user's identity. Techopedia

Auditability: The ability to produce a chain of evidence in the form of hard or electronic business transactions or communications resulting from business processes, functions or programming executions. Derived from Dictionary and Techopedia.

Bandwidth Consumption: For this paper; the act of consuming or using the bit-rate measure of the transmission capacity over a network communication system.

BOTs: A device or piece of software that can execute commands, reply to messages, or perform routine tasks, as online searches, either automatically or with minimal human intervention. Dictionary.com

Chief Information Officer: An individual that manages an organization's technology and IT interdepartmental manager communications and is responsible for strategizing and facilitating improvement within the organization. Techopedia

Combatant Commands: A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. DOD Dictionary of Military and Associated Terms, May 2017.

Common View: Consensus of common objectives, a common operating environment, and common categories of effort by stakeholders and mission partners. Unity of Effort Solution Guide, 2013

Common Understanding: Consensus by mutual agreement on joint activity or settling differences. Derived from Oxford dictionary and Unity of Effort Solution Guide, 2013

Communication Security: Communications security (COMSEC) ensures the security of telecommunications confidentiality and integrity - two information assurance (IA) pillars. Generally, COMSEC may refer to the security of any information that is transmitted, transferred or communicated. Techopedia

Configuration Management: System or process used to keep track of an organization's hardware, software and related information. Techopedia

Cyber: Relating to or characteristic of the culture of computers, information technology, and virtual reality. Oxford Dictionary

Cyber-Attacks: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. National Institute for Standards and Technology, US Department of Commerce, NISTIR 7298, Revision 2, 2013

Cyber Criminal: An individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both. Techopedia

Cyber Espionage: A cyber operation to obtain unauthorized access to sensitive information through covert means. East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014, - 2014

Cyber Threats: The possibility of a malicious attempt to damage or disrupt a computer network or system. Oxford Dictionary

Cyber Threat Information: Any information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face. NIST SP 800-150.

Data Center: A repository that houses computing facilities like servers, routers, switches and firewalls, as well as supporting components like backup equipment, fire suppression facilities and air conditioning. Techopedia.

Data Confidence: For this paper; Confidence in the fact that the data/information is accurate and current.

Denial-of-Service: Any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. Techopedia.

Designated Approval Authority: Individual appointed as the approval authority for any activity, modifications, or changes to an organizational network.

Enterprise Architecture: A specialist that works closely with stakeholders, including management and subject matter experts (SME), to develop a view of an organization's strategy, information, processes and IT assets. Techopedia

Federated Connection: A IT connection from one network or organization to another network or organization for the purposes of sharing or passing information/data.

Framework: A mechanism that allows government agencies to visualize and preempt or resolve potential conflicts in their actions, activities and resources in order to support a specific national strategy or policy. Unity of Effort Solution Guide, 2013

Hardware: Physical elements that make up a computer or electronic system and everything else involved that is physically tangible. Techopedia

Identification: The act or instance of identifying; the state of being identified or verifying who you are. Dictionary.com

Information Assurance: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. National Institute for Standards and Technology, US Department of Commerce, NISTIR 7298, Revision 2, 2013

Information Leakage: For this paper; the accidental or purposeful spillage of data/information to someone or a something like a network.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. National Institute for Standards and Technology, US Department of Commerce, NISTIR 7298, Revision 2, 2013

Intrusion Detection System: An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations. Techopedia

Inhibitor: Reasons, rationales, and explanations, which impede unity of effort. Unity of Effort Solution Guide, 2013

Limited Network Access: For this paper; the limited ability to gain access to an authorized network.

Malicious User: For this paper; a user with intent to do willful, intentional harm to an information system.

Memory Consumption: For this paper; the use of any information or data, often in binary format, that a machine or technology can recall and use.

Mobile Environment: For this paper; business practice of using mobile platforms to get core operations done.

Network: A system containing any combination of computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables: used to transmit or receive information. Dictionary.com

Network Administrator: For this paper; an individual that manages an organization's network.

Network Latency: Term used to indicate any kind of delay that happens in data communication over a network. Techopedia.

Network Security: An over-arching term that describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources. Techopedia

NIST: National Institute of Standards and Technology

NATO: North Atlantic Treaty Organization

National Security Agency: The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances. NSA

Phishing Attack: Fraudulent act of acquiring private and sensitive information, such as credit card numbers, personal identification and account usernames and passwords and account access via deceptive methods. Derived from Techopedia.

Remote Access System: A system that provides the ability to access a computer, such as a home computer or an office network computer, from a remote location. Derived from Techopedia.

Software: A set of instructions or programs instructing a computer to do specific tasks. Software is a generic term used to describe computer programs. Scripts, applications, programs and a set of instructions are the terms often used to describe software. Techopedia.

Trojan: A seemingly benign program that when activated, causes harm to a computer system. Techopedia.

Unity of Effort: Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization. The product of successful unified action. [Ref: JP-1] A cooperative concept, which refers to coordination and communication among USG organizations toward the same common goals for success; in order to achieve unity of effort. It is not necessary for all organizations to be controlled under the same command structure, but it is necessary for each agency's efforts to be in harmony with the short- and long-term goals of the mission. Unity of effort is based on four principles [Ref: DOS]:

- Common understanding of the situation
- Common vision or goals for the R&S mission
- Coordination of efforts to ensure continued coherency
- Common measures of progress and ability to change course if necessary

Virtual Desktop Infrastructure: A virtualization technique enabling access to a virtualized desktop, which is hosted on a remote service over the Internet. It refers to the software, hardware and other resources required for the virtualization of a standard desktop system. Techopedia

Worms: A type of malicious software (malware) that replicates while moving across computers, leaving copies of itself in the memory of each computer in its path. Techopedia.

Appendix B: References

A. 19th ICCRTS A Methodology to Improving Unity of Effort for Mission Partner Planning paper 003 - 17 June 2014
B. DOD, DOD Dictionary of Military Terms and Definitions, 2017
C. DOD, DODI 8500.01, Cybersecurity, 14 March 2014
D. DOD, Joint Staff J7, Unity of Effort Framework Solution Guide, Aug 2013
E. NATO, Primary Directive on CIS Security, AC/35-D2004-REV3, 15 Nov 2013.
F. NATO, Security Within the North Atlantic Treaty Organisation, C-M(2002)49-COR9, 5 Feb 2013.
G. NATO, The Management of Non-Classified NATO Information, C-M(2002)60, July 2002.
H. NIST, Guide to Cyber Threat Information Sharing, National Institute of Standards and Technology, NIST SP 800-150.
I. NIST, Information Security Continuous Monitoring for Federal Information Systems and Organizations, National Institute of Standards and Technology, SP 800-137, 2011
J. NIST, US Department of Commerce: Glossary of Key Information Security Terms, June 2013
K. Mark von Rosing, August-Wilheim Scheer, Henrik von Scheel, The Complete Business Process Handbook, 2015 LEADing Practice ApS
L. USG, Circular No A-130, Managing Information as a Strategic Resource, July, 2016.