ESSA

CREATE SHARE ENHANCE

“During a significant cyber event, no single entity will have all the information, authorities, and/or capabilities to enable comprehensive action!”

ENHANCE SHARED SITUATIONAL AWARENESS

The overall classification of this briefing is UNCLASSIFIED

Information Sharing Architecture (ISA): Framework Introduction and Requirements Discussion

19 December 2013

AGENDA

- Problem Space
- Information Sharing Architecture (ISA)
  - Evolution
  - Functions
  - Enduring Functional Exchanges (EFE)
- Share Situational Awareness Requirements
  - Use Cases
  - Operational State
  - Mission, Technology, and Information
- Challenges
- Partnership Engagement
- Way Ahead

PROBLEM WE'RE TRYING TO ADDRESS?

- Our individual efforts fall short of meeting our collective needs and expectations for integrated operational action

- One of the keys to increasing security and resilience is enhancing our cyber shared situational awareness

ESSA

CREATE SHARE ENHANCE

ENHANCE SHARED SITUATIONAL AWARENESS

Information Sharing Architecture – Framework Evolution, Functions, and EFEs

ESSA INFORMATION SHARING ARCHITECTURE (ISA)

- Creating Shared Situational Awareness is primarily a policy, information and analytic-based challenge, not an IT challenge

- Developed an approach that:
  - De-couples ‘functional’ from ‘physical’ organizations
  - Designed to work at machine speed
  - Anticipates/enables extensibility
  - Accommodates policy/authority considerations
  - Establishes the blueprint

ISA Evolution

- December 2010 – Published the **Information Sharing Architecture (ISA): Framework**
- April 2011 – **As-Is Definition and Assessment** of current information sharing activities among participants
- July 2011 – participant-designed mission threads/table top exercises to refine ISA definitions
- March 2012 – **ISA Desktop Reference Guide** published (in revision)
- May 2012 – **National Level Use Cases**, developed and exercised
- November 2012 – **Implementation Working Group** chartered
- December 2012 – **Policy Working Group** chartered
- July 2013 – Published the **ISA: Technical Implementation Plan (TIP) v1.0**
- October 2013 – Published the **ISA: Shared Situational Awareness (SSA) Requirements Document v2.1** (Mission Technology, and Information)
- Integrated efforts into the EO 13636 and PPD21 solutions

ISA Functions

Network Operations Function (NOF)

NOF

- Infrastructure Operations and Management
- Configuration Management
- Risk ID, Management, and Reduction
- Certification and Accreditation

Computer Network Defense Function (CNDF)

CNDF

- Detection and Mitigation
- Remediation
- Focused Vulnerability Assessment

Domain/Sector Awareness Function (D/SAF)

D/SAF

- Status Aggregation and Reporting
- Risk Assessment
- Information Validation and Dissemination

Threat Assessment Function (TAF)

TAF

- Incident and Threat Discovery
- Threat Characterization and Assessment
- Forensics and Malware Analysis
- Mitigation and Signature Development
- Indicator and Warning Development

Threat Operations Function (TOF)

TOF

- Ops Planning and Execution
- Characterization of achievable reach and effects
- Damage and Consequence Assessment

Integrated Operational Action Planning Function (IORPF)

IOAPF

- Course of Action Development and Selection
- Mitigation Planning (Pre-emptive and Responsive)
- Equities Assessment

Integrated Operational Action Coordination Function (IORCF)

IOACF

- Action activation and tracking
- Integrated coordination and reporting
- Effectiveness Assessment (Operations and Mission Level)

ISA Enduring Functional Exchanges (EFE)

1 Configuration/Anomaly Reporting

- Infrastructure Information
- Risk Posture
- Anomalies

2 Knowledge of Threat Actors

- Threat Actor Infrastructure
- Threat Actor Personas
- Collected Threat Actor Indicators
- Threat Actor Attribution
- Trend Analysis
- Victim Information

3 Incident Awareness

- Incident Information
- Incident Data
- Infrastructure Impact and Effects
- Investigations/cases
- Alerting Indicators
- Victim Information

4 Indications and Warnings

- Events and Alerts
- Tipping and Cueing
- Warnings
- Impact assessments
- Potential Indicators

5 Vulnerability Knowledge

- Vulnerabilities
- Exploits
- Potential Victim Information

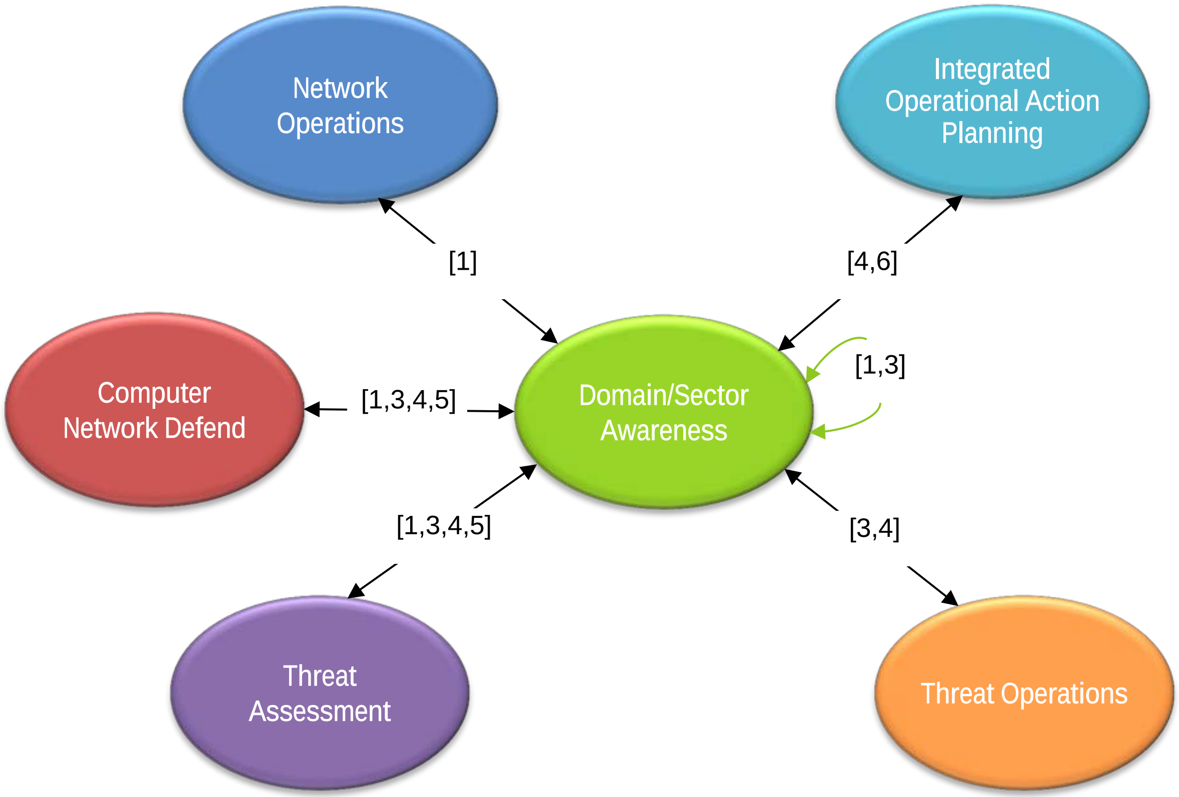
6 Mitigation Strategies

- Coordinated Action Plans
- Courses of Action
- Understanding of Achievable Mitigation Effects

7 Mitigation Actions and Responses

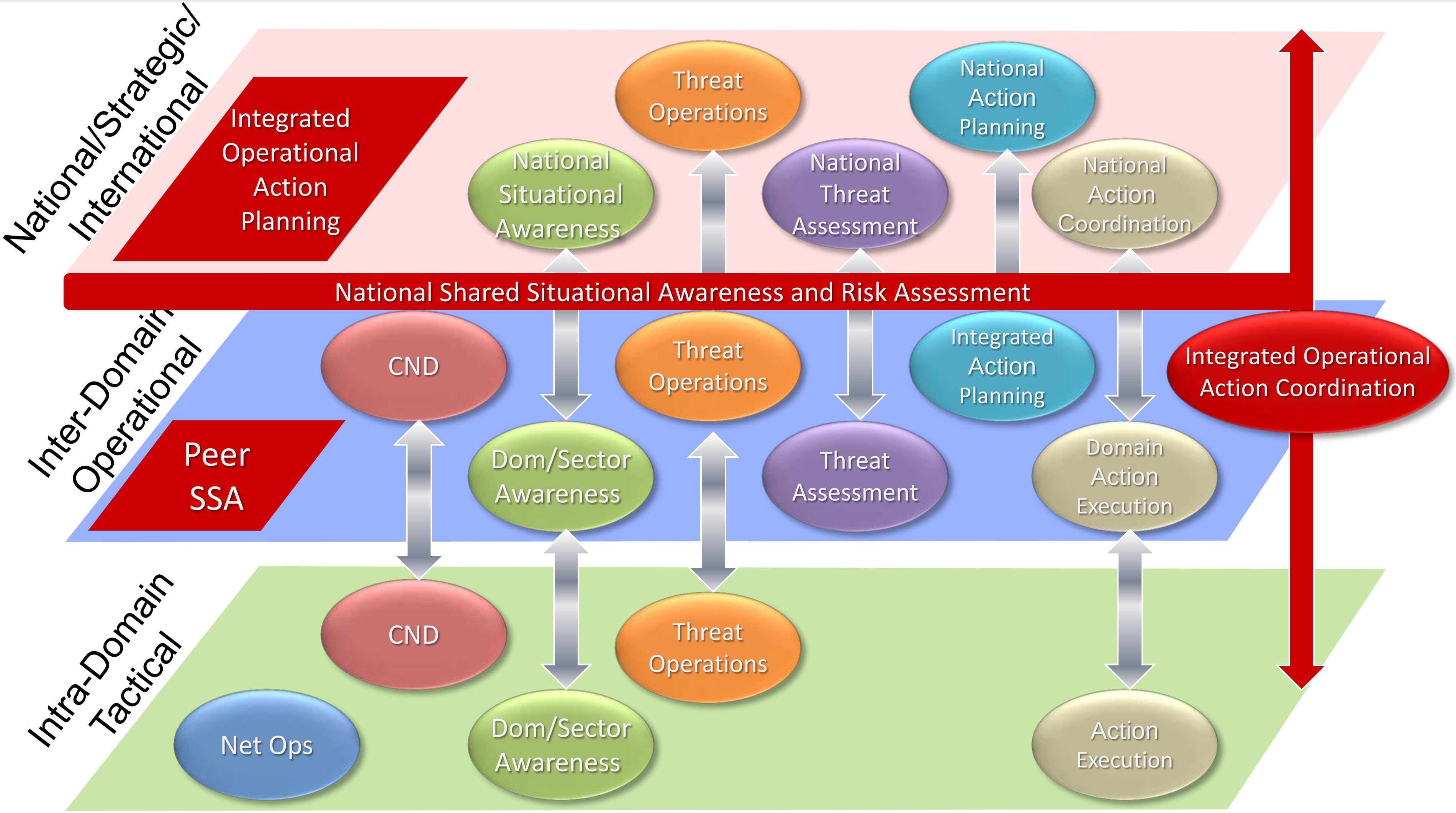
- Computer Network Operations (CNO) Awareness
- Action Tasking and Status
- Effectiveness Reporting
- After Action Reporting and Lessons Learned

Domain/Sector Awareness Function



Domain/Sector Awareness Function associated EFEs:
(1) Configuration/Anomaly Reporting
(3) Incident Awareness
(4) Indications and Warnings
(5) Vulnerability Knowledge
(6) Mitigation Strategies

ISA Applies Between and Among Mission/Operational ‘Levels’


National/Strategic/ International
Integrated Operational Action Planning
Threat Operations
National Action Planning
National Situational Awareness
National Threat Assessment
National Action Coordination
National Shared Situational Awareness and Risk Assessment
Inter-Domain Operational
CND
Threat Operations
Integrated Action Planning
Integrated Operational Action Coordination
Peer SSA
Dom/Sector Awareness
Threat Assessment
Domain Action Execution
Intra-Domain Tactical
CND
Threat Operations
Net Ops
Dom/Sector Awareness
Action Execution

ESSA

CREATE SHARE ENHANCE

ENHANCE SHARED SITUATIONAL AWARENESS

Information Sharing Architecture (ISA) – Requirements (Mission, Technology, & Information)

ISA REQUIREMENTS INTRODUCTION

- The requirements document gives the checklist to implement the ISA capabilities to support your mission.

- The requirements are the result of an analysis of the functions and EFEs, participant-led capability self assessments, developed use cases, and operational SME input.

- For specific solution implementations the participants will further refine, decompose, and allocate the requirements

The ISA Requirements – Supporting the Use Cases

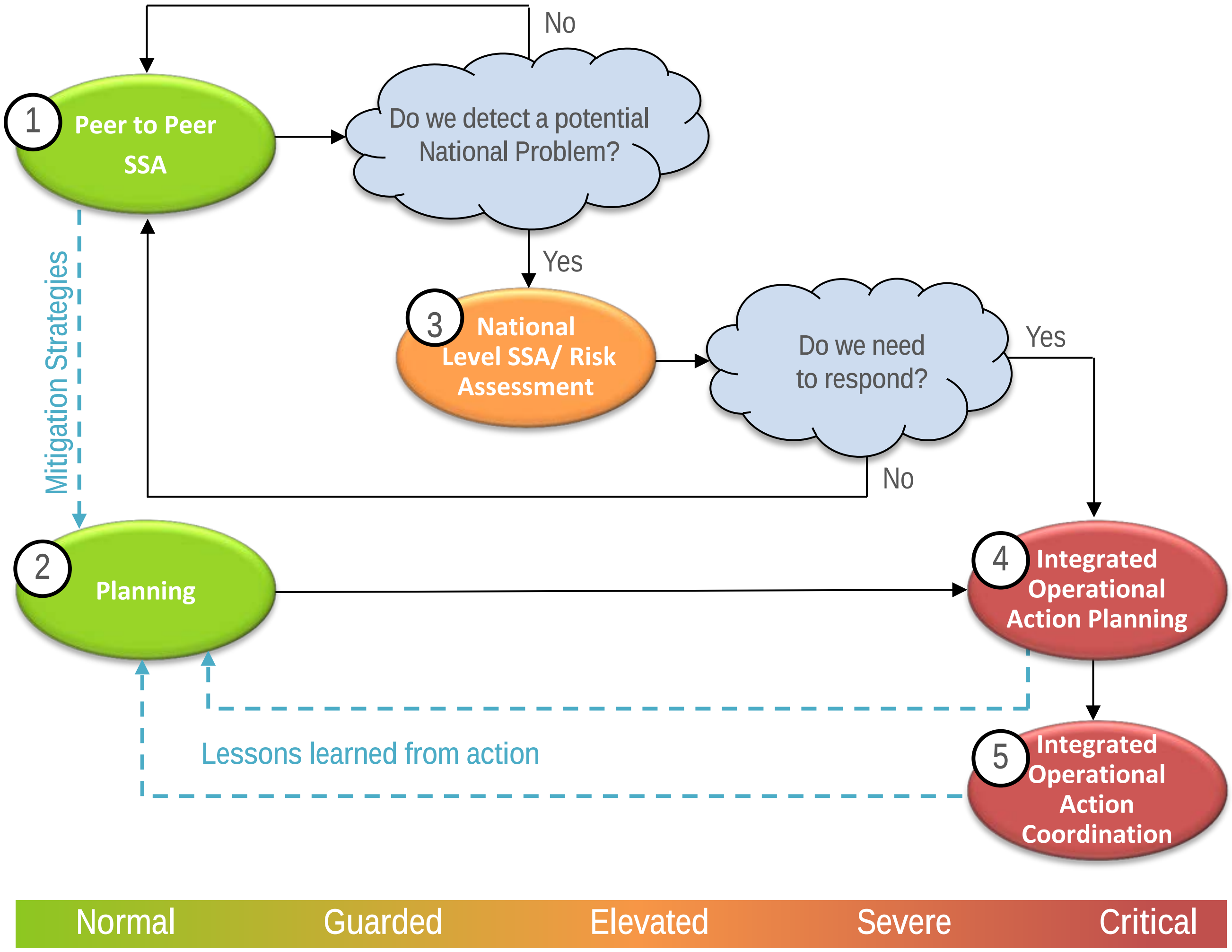
- Lessons learned during the development
  - Requirements are not just technical but must address mission and information
  - Set the context – Mission
  - Describe the what – Technical
  - Describe the what exchanged - Information

Mission Use Cases – Req. Doc. Pg. 8

Use Case Area	Description
Peer Shared Situational Awareness (SSA)	The exchanges and collaboration among partners, and other participants that enable each of the participants to improve functions within their own domains.
Planning	The creation of general action plans by each center for threats within their scope. For centers that have the authority to address national – level Action, national level planning would be included as well.
National Level (SSA)/ Risk Assessment	The process of determining whether or not a threat requires an Integrated Operational Action.
Integrated Operational Action Planning	Activities that include the development and refinement of COAs, assessment of equity considerations, and implementation of national policy.
Integrated Operational Action Coordination	Activities that involve the execution of the plans developed such that each Center executes its part of the plan according to its capabilities and authorities, coordination, workflow management, and post-Action assessment of effectiveness need to be enabled.

Relationship Between Use Cases and Operational State

Identified additional Data Exchanges


No
1
Peer to Peer SSA
Do we detect a potential National Problem?
Yes
3
National Level SSA/ Risk Assessment
Do we need to respond?
Yes
No
Mitigation Strategies
2
Planning
4
Integrated Operational Action Planning
5
Integrated Operational Action Coordination
Lessons learned from action
Operational State
Normal
Guarded
Elevated
Severe
Critical

Mission Requirements- Req. Doc. Pg. 17

Why are we sharing, traced to use case

			Trace to Use Case Steps			
MR #		Mission Requirement Description	Peer SSA	National SA and RA	IOR Planning	IOR Coordination
MR-31	(U)	ISA Participants shall use other Participants' countermeasure information, as appropriate to their mission needs, for activities such as determining if they need to apply the same or similar countermeasures.	28, 30, 32, 36			
MR-32	(U)	ISA Participants shall make available information, as appropriate to their mission, associated with current and planned Computer Network Operations (CNO) operations, relevant to the other Participants' operations.		2		
MR-33	(U)	ISA Participants shall use other Participants' reported CNO operations information, as appropriate to their mission needs, to avoid classifying these activities as malicious.		2		
MR-34	(U)	ISA Participants shall, when appropriate, make available for sharing an anticipated increase of activity due to Threat Operations.		2		
MR-35	(U)	ISA Participants shall make available, within the authorities governing their operations, information that will permit a national, strategic understanding of the scope of the event and enable more effective tactical and strategic decision-making.	All			
MR-36	(U)	ISA Participants assigned national, strategic decision making responsibilities shall request and use, where appropriate to their mission, information provided by ISA Participants to enhance their mission.	All			

Technology Requirements – Trusted Identity – Req. Doc. Pg. 27

What will the ISA do to verify the identity, both people and systems

Contains requirements for both Participants (P) and Service Providers (S)

TR-21	(U)	The access control mechanism for shared resources shall be decentralized (i.e., distributed among the information sharing ISA Participants) rather than the responsibility of a centralized authority.	S/P
TR-22	(U)	The sharing infrastructure shall include an agreed-upon trust model for information exchange.	S/P
TR-23	(U)	The access control mechanism shall authenticate users and NPEs in Unclassified environments.	S/P
TR-24	(U)	The access control mechanism shall authenticate users and NPEs in a Secret environment.	S/P
TR-25	(U)	The access control shall authenticate users and NPEs in a Top Secret environment.	S/P
TR-26	(U)	Access control mechanisms at each classification level shall utilize Levels of Assurance (LOAs) appropriate to local security policies.	S/P
TR-27	(U)	The access control mechanisms shall be capable of accepting multiple types and forms of identity credentials [including Department of Defense (DoD) CAC, PIV, and PIV-I] by leveraging a PKI trust relationship.	S/P

Technology Requirements – Access Control – Req. Doc. Pg. 29

What will be Done to Ensure That Information is Accessed by Authorized Parties

TR-36	(U)	Access control mechanisms shall limit access according to the information control metadata associated with each information element, applications, services or analytics and the authorization attributes of the user (see Section 4.3).	S
TR-37	(U)	Access control mechanisms shall not reveal the existence of information to which access is being denied based on attribute settings.	S
TR-38	(U)	Each ISA Participant shall define baseline access control attribute settings in accordance with the authorities and policies governing their operations.	P
TR-39	(U)	The access control mechanism shall be able to track when results from a common analytic were not released due to attribute-based controls.	S

Technology Requirements – Applications - Req. Doc. Pg. 32

What Applications will the ISA deliver

TR-65	(U)	The ISA application suite shall include the capability for the user to define an operational picture to enhance situational awareness.	S
TR-66	(U)	The ISA application suite shall include a CIR capability that supports the tracking and alerting of CIR status across multiple Participants.	S
TR-67	(U)	ISA application suite shall include a Workflow Management capability to support IOA coordination across multiple Participants in one workflow.	S
TR-68	(U)	ISA application suite shall include a Workflow Management capability that supports user-definable workflows.	S

Information Requirements – Req. Doc. Pg. 34

The WHAT EXCHANGED–
Based on self-identified functions

D/SAF

IR-3

(U) All ISA Participants with a Domain/Sector Awareness Function/Mission shall make available the following data when it is produced and determined to be appropriate for ISA sharing:

- (U) *Risk Posture (1a)*
- (U) *Victim Information (2e)*
- (U) *Incident Information (3a)*
- (U) *CNO Awareness (3b)*
- (U) *Incident Data (3c)*
- (U) *Infrastructure Impact/Effects (3d)*
- (U) *Warnings (4b)*
- (U) *Impact Assessments (4c)*
- (U) *Potential Indicators (4d)*
- (U) *Vulnerabilities (5a)*
- (U) *Exploits (5b)*
- (U) *Understanding of Achievable Mitigation Effects (6c)*

ESSA

CREATE SHARE ENHANCE

ENHANCE SHARED SITUATIONAL AWARENESS

Challenges

(U) Non-Technical Information Sharing Challenges

(U) Protected Categories of Information

- Law Enforcement
- Intelligence
- Personally Identifiable Information (PII)
- Protected Critical Infrastructure Information (PCII)
- Proprietary
- Sensitive But Unclassified
- Unclassified For Official Use Only

(U) Areas of Concern for System-to-System Sharing

- Co-mingling of data
- Usage/Handling/Dissemination authorities
- Releaseability
- Certification & Accreditation
- Data protection
- Classification/Spillage
- Data aggregation/Purging
- Certification &Training Standard

ESSA Policy Working Group (PWG) Overview

- The PWG is chartered to identify and, whenever possible, solve the policy challenges to multi-partner cybersecurity information sharing. A particular focus of the PWG will be net-speed (machine-to-machine) information sharing.
  - *The scope is limited to cybersecurity information sharing at machine speed.*
- Multiple participants drawn from organizations supporting the Federal cybersecurity centers

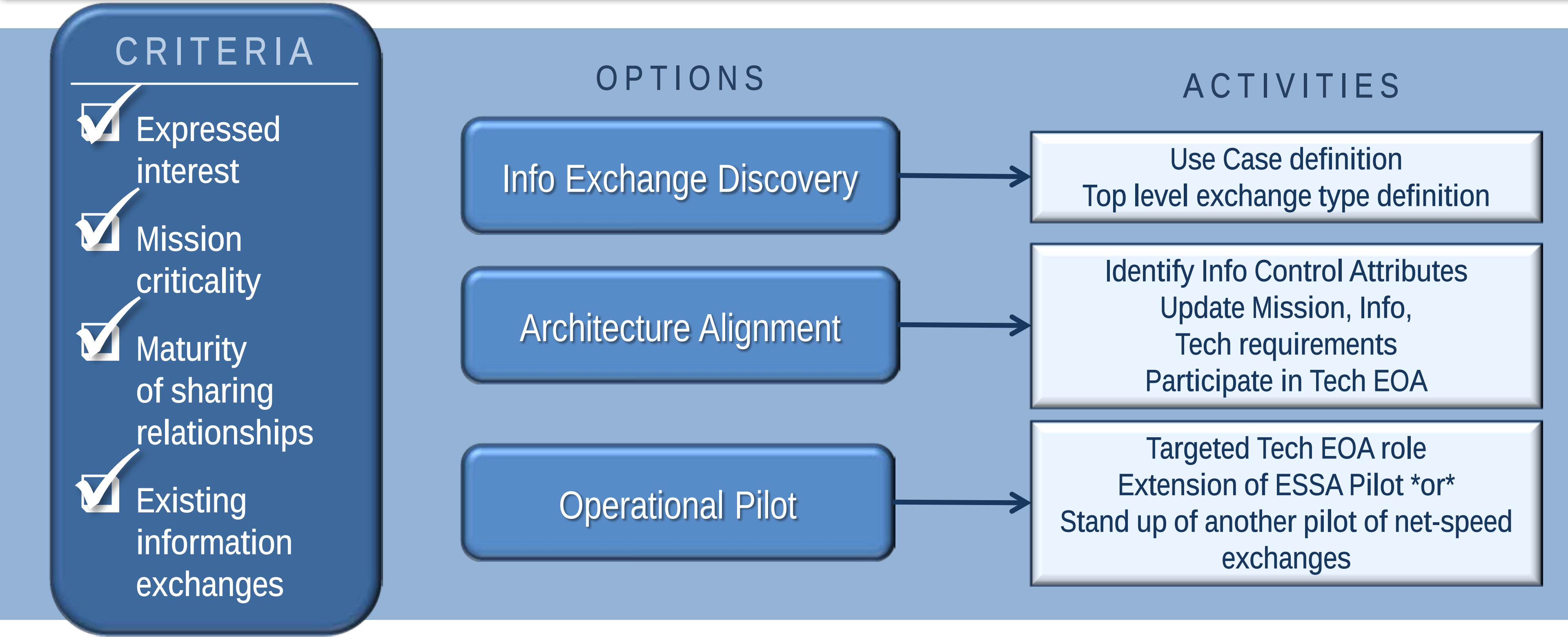
ESSA

CREATE SHARE ENHANCE

ENHANCE SHARED SITUATIONAL AWARENESS

Partnership Engagement: A Strategy

Partner Engagement Process



CRITERIA

- ☑ Expressed interest
- ☑ Mission criticality
- ☑ Maturity of sharing relationships
- ☑ Existing information exchanges

OPTIONS

Info Exchange Discovery

Architecture Alignment

Operational Pilot

ACTIVITIES

Use Case definition
Top level exchange type definition

Identify Info Control Attributes
Update Mission, Info,
Tech requirements
Participate in Tech EOA

Targeted Tech EOA role
Extension of ESSA Pilot *or*
Stand up of another pilot of net-speed exchanges

- Partner can participate in any one or more activities (from top down)
- Engagement could evolve to other activities
- Capture lessons learned to ease future engagement
- Integrate and derive products where necessary

ESSA

CREATE SHARE ENHANCE

ENHANCE SHARED SITUATIONAL AWARENESS

The Way Ahead

Where We Need to Go

- Sustained emphasis on Net-speed sharing parsable and discoverable @ machine-speed
- Trusted analytics
- Move beyond bi-lateral information sharing (organizational focus) to multi-lateral information sharing (information focus)
- Robust participation in design and development
- Early piloting/capability delivery
- Go operational in steps, as fast as partners are willing & able
- Expand to other partners

CONTACT US

Antonio “T” Scurlock, DHS

Portfolio Management Team (PMT)

Enhance Shared Situational Awareness (ESSA)

William “Bill” Jones, FBI

Portfolio Management Team (PMT)

Enhance Shared Situational Awareness (ESSA)

Robin DeStefano, NSA

Portfolio Management Team (PMT)

Enhance Shared Situational Awareness (ESSA)

ESSA

CREATE SHARE ENHANCE

ENHANCE SHARED SITUATIONAL AWARENESS

DISCUSSION