

Federal Multilateral Information Sharing Agreement January 2019

Purpose:

The purpose of this cross-government Multilateral Information Sharing Agreement (MISA), herein referred to as the “Agreement,” is to enhance cybersecurity information sharing among federal agencies in order to better protect the United States from malicious cyber actors in a manner that is fully consistent with the Constitution and laws of the United States, Executive Orders and other Executive Branch directives and policies, court orders, and all other legal, policy, and oversight requirements.

Implementation of this Agreement facilitates improved cyber shared situational awareness across all classification domains, by utilizing machine-speed sharing of cybersecurity information and data as originally defined by the Enhance Shared Situational Awareness (ESSA) Information Sharing Architecture (ISA) Framework within the Comprehensive National Cybersecurity Initiative Five (CNCI-5) *ISA Phase 1 Document, v1.0* (REF A) and integrated operational action within and across the Federal Government.

Scope:

To better ensure the sharing of timely, accurate, and informative cybersecurity information, this Agreement establishes cybersecurity information sharing responsibilities for Federal Government participant organizations, including both current participants¹, and any acceded departments and agencies, herein referred to as Federal Information Sharing Participants. Participants to the Agreement intend to share information and data for authorized U.S. Government cybersecurity purposes as defined by the ISA Functions within the document, *ISA Shared Situational Awareness Requirements, v2.1* (REF B) and listed in Annex A. Cybersecurity information and data is also intended to be used and shared for any other authorized national security or law enforcement purpose unless further restricted in response to governing laws, policies, or classification determinations. Sharing of information and data will also support the policy objectives set forth in PPD-21, “*Critical Infrastructure Security and Resilience*” (REF C), EO 13636, “*Improving Critical Infrastructure Cybersecurity*” (REF D), and *Cybersecurity Information Sharing Act of 2015* (CISA) (REF H and supporting guidance H1 – H4).

This Agreement does not create legally enforceable rights between Federal Information Sharing Participants. It does not supersede any Federal Information Sharing Participants’ existing cybersecurity information sharing agreements, nor does it preclude any Federal Information Sharing Participant from entering into information sharing agreements outside the MISA. In cases where future cybersecurity information sharing agreements are established, such agreements should reflect, to the greatest extent possible and appropriate, the guidance and approach contained in this Agreement.

References (including future revisions) ²:

REF A: CNCI-5 ISA Phase 1 Document, v1.0, 30 September 2011

REF B: ISA Shared Situational Awareness Requirements, v2.1, 21 October 2013

¹ See Annex C for list of current Federal Government participating organizations.

² The documents can be viewed electronically via OMBMAX:
<https://community.max.gov/pages/viewpage.action?pageId=1615373314>

REF C: Presidential Policy Directive (PPD)-21, Critical Infrastructure Security and Resilience, February 2013

REF D: Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, February 2013

REF E: Summary of Conclusions (SOC): Kickoff Meeting for FY2014 Passback Cyber Information Sharing Task, February 15, 2013

REF F: National Strategy for Information Sharing and Safeguarding, December 2012

REF G: ACS Marking Definition Version 3.0 - STIX™ Version 2.1. Part 1: STIX, Version 1.0, October 2018

REF H: Cybersecurity Information Sharing Act, December 2015

REF H1: Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, June 15, 2016

REF H2: Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015, June 15, 2018

REF H3: Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015, February 16, 2016

REF H4: Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government, June 15, 2016

REF I: ISA Technical Implementation Plan, v2.0, March 24, 2014

REF J: Information Sharing Architecture (ISA) Access Control Specification (ACS), Version 3.0, February 2016

REF K: Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2017

Authorities:

This Agreement is entered into pursuant to: NSPD-54/HSPD-23, “*Cybersecurity Policy*,” dated January 2008; REF C; REF D; and REF H, as applicable to particular sets of information. Federal Information Sharing Participants operate under their own authorities while working to build trusted information sharing relationships through the implementation of the ISA. Information sharing activities will be conducted in full compliance with Federal Information Sharing Participants’ authorities and statutory and regulatory requirements while protecting privacy, civil rights, and civil liberties. No authorities are generated, created, or transferred as a result of this Agreement.

Background:

The vision for cross-government cybersecurity information sharing is to create cybersecurity shared situational awareness that enables integrated operational action. This Agreement responds to the Office of Management and Budget (OMB) and the National Security Council (NSC) staff action to establish an information sharing system that supports machine-to-machine cybersecurity information sharing among all agencies in the Federal Government (see REF E). This Agreement aligns with Priority Objective 2 of the *National Strategy for Information Sharing and Safeguarding* (REF F): “Develop guidelines for information sharing and safeguarding agreements to address common requirements, including privacy, civil rights, and civil liberties, while still allowing flexibility to meet mission needs.”

Participation:

Federal Information Sharing Participants commit to work collaboratively on sharing information and data and/or providing capabilities that meet the information, mission, and technical requirements outlined in REF B and REF H (and supporting guidance H1 – H4), where the latter is specifically invoked with respect to a particular set of information. Federal Information Sharing Participants perform ISA Functions, such as Network Operations and Threat Assessment (see Annex A), and exchange cybersecurity information, regarding incidents, malware, and threat actors (see Annex B) as part of their respective cybersecurity missions. Federal Information Sharing Participants may have one or more roles, as follows:

- **Data Producer:** Organization that has agreed to make unclassified, secret, or top secret information and data available from its repositories.
- **Data Consumer:** Organization that consumes data shared by Data Producers.
- **Shared Capability Provider:** Organization that provides ISA-compatible technical solutions to multiple Federal Information Sharing Participants (i.e. the service provider for Data Consumers to access Data Producers' information and data). The Shared Capability Provider may also lead multiple working groups (i.e. technical, access controls, etc.) in addition to potentially providing the back-end software, subject to license restrictions, that accesses each Data Producer's repository.

Roles and Responsibilities:

All Federal Information Sharing Participants will implement this Agreement in a manner that: (a) is fully consistent with the Constitution and laws of the United States, Executive Orders and other Executive Branch directives and policies, court orders, and all other legal, policy, and oversight requirements; and (b) protects the data that is shared from unauthorized access, disclosure, and compromise. Accordingly, all Federal Information Sharing Participants will develop and implement appropriate data access controls, other data handling and dissemination controls, and auditing functions to maintain ISA compliance in accordance with REF B, REF G, REF H (and supporting guidance H1 – H4) to the extent that CISA is invoked with respect to a particular set of information, REF I and REF J, protect against internal and external threats and misuse, and ensure due regard for agencies' privacy, civil rights, and civil liberties obligations.

Data Producers shall:

- Identify access controls and other relevant data handling and dissemination controls required to share and protect their data in accordance with their organization's legal, policy, and compliance requirements.
- Whenever possible, share information and data with as few restrictions as possible.
- Enable appropriate access to information and data by tagging data with access, handling, and usage controls in accordance with REF J.
- Be accountable for ensuring Shared Capability Provider services enable Data Producers to meet the legal, policy, and notification requirements for the information and data they share.
- Identify systems security standards, data protection standards, and best security practices that Federal Information Sharing Participant information systems must meet to responsibly share their data consistent with Data Producers' legal and policy requirements.

- Make shared information and data available via ISA-compliant³ mechanisms as identified in REF B and REF I.
- When training is required, make training available to those Data Consumers authorized to receive information or data.
- Retain their existing records management, and legal, regulatory, and policy responsibilities for the information and data they provide in accordance with this Agreement.

Data Consumers shall:

- Abide by laws, regulations, and U.S. Government policy governing information and data they may receive, access, or view by virtue of participating in cross-government information sharing (consistent with Data Producers' legal, policy, and notification requirements).
- Adhere to legal and policy requirements (established through tagging) of the information or data they receive, and for their subsequent use and sharing of that information or data, to include queries, running analytics, and end-product generation.
- Use shared information and data only inside of its designed access usage and dissemination controls, unless expressly permitted by the Data Producer in accordance with applicable laws and internal regulations, procedures, or agreements.
- Provide user attributes to Shared Capability Providers to enable access and authorization decisions to Data Producers' shared information in compliance with REF J requirements.
- Access only those data elements that match their access control attributes.
- Take the necessary training required prior to accessing information or data.
- Provide Data Producers' requirements on the handling, retention, dissemination, and use of information or data to any authorized organization with which they share information or data acquired under this Agreement.
- Consult with the appropriate Data Producer regarding legal processes (e.g., complaints, subpoenas, warrants, and other legal processes) and adhere strictly to all applicable legal requirements.
- Agree to make all reasonable efforts to purge or delete shared information or data when requested by Data Producer and to pass along such requests if the information or data is shared beyond the Data Consumer.

Shared Capability Providers shall:

- Provide system controls that ensure Data Consumers have access to only those data elements that match their access control attributes as specified by Data Producers.
- Consult with the appropriate Data Producer regarding legal processes (e.g., complaints, subpoenas, warrants, and other legal processes) served upon the Shared Capability Provider concerning the Data Producer's data.
- Agree to make all reasonable efforts to purge or delete shared information or data when requested by Data Producer and to pass along such requests if the information or data has been shared.
- Ensure that all systems security and data protection standards are met.
- Ingest ISA-compliant data and make that data available to Data Consumers in accordance with the access controls designated by Data Producers.

³ Information and/or data that is formatted in terms of community agreements (e.g., STIX and TAXII) and ingested or further disseminated in accordance with an agreed upon data tagging specification (i.e., ACS).

- Employ data protection methodologies using data tagging that includes access controls, compliance requirements, and handling controls that facilitate data sharing while protecting data from inadvertent exposure; or pass appropriate information or data to Data Producers to enable them to perform data access control (consistent with Data Producers' legal, policy, and notification requirements).
- Handle information and data in accordance with the controls and processes identified by Data Producers, and coordinate with Data Producers regarding requests to purge or delete information or data.
- Employ and actively monitor an audit tracking function to record, retrieve, and store accesses, changes, or deletions to shared data and to track authentication and authority data, creating an audit trail for maintenance purposes.

Shared Capability Providers will not:

- Be responsible for the accuracy or quality of Data Producers' data.
- Be liable for the loss of data due to system outages or catastrophic events, unless they explicitly assume such responsibilities in subsequently executed agreements.

There may be types of information or data exchanged, such as malware, which may require additional technical security protections. These protections will be agreed among Federal Information Sharing Participants.

Every Federal Information Sharing Participant will identify a point-of-contact (i.e., an office or individual) that can be contacted by other Federal Information Sharing Participants regarding authentication control, legal, and information assurance purposes. The list will be maintained by the DHS in a location accessible to all Federal Information Sharing Participants.

Compliance:

This Agreement shall be implemented in compliance with all applicable law, policy, and other guidance, including those that protect privacy, civil rights and civil liberties. All Federal Information Sharing Participants are responsible for ensuring that their respective systems are designed, managed, and operated in compliance with all relevant laws, regulations, and policies.

Funding:

No appropriated funds are obligated by this Agreement, nor does it transfer or exchange authorized manpower between the Participants. Expenditures by each Federal Information Sharing Participant will be subject to its acquisition and budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. Federal Information Sharing Participants acknowledge that the language in this Agreement in no way implies that funds will be made available for such expenditures.

Record Keeping:

DHS will maintain signed copies of this Agreement and its respective annexes. Federal Information Sharing Participants are responsible for any internal record keeping requirements.

Updates, Review, and Termination:

This Agreement becomes effective for each Federal Information Sharing Participant upon that Participant's signature.

This Agreement is designed to be flexible and enduring. Occasionally updates and/or changes may be required. The following processes shall be followed to support proposed updates or changes to this agreement.

Administrative Update:

Administrative updates are modifications to the Agreement that clarify or update accuracy of content over time and are within scope of the Agreement. Administrative updates can be identified by Participant policy representatives and incorporated by DHS as part of this Agreement without negating the original Agreement. The process for incorporating an administrative update is as follows:

1. Participants identify an administrative update;
2. Participants e-mail recommended administrative update to DHS (see Points of Contact section below);
3. DHS reviews recommended administrative update to confirm the update only clarifies or updates accuracy of existing content and is within scope of the original Agreement.
4. If DHS is in agreement, DHS will make the administrative update to the MISA and forward the updated Agreement to all Participants.

Changes Other Than Administrative:

Changes deemed other than administrative by Participant policy representatives may require that Federal Information Sharing Participants re-sign the updated Agreement. DHS will manage this process and make an earnest attempt to reach consensus.

Participant consensus is preferred for a change other than administrative to be considered and incorporated. When a change other than administrative is identified, DHS will identify a subset of Federal Information Sharing Participants, to include representatives from the MISA initial seven signatories on Page 8, to form a Policy Working Group (PWG) to review and consider recommended changes that are other than administrative. The PWG will act as representation for all Participants. If the PWG reaches a consensus regarding the recommended change, the change can be implemented. The process for incorporating changes other than administrative is as follows:

1. Participants identify a change other than administrative;
2. Participants e-mail recommended change to DHS (see Points of Contact section below);
3. DHS forms a PWG to review and consider the recommended change;
4. If the PWG reaches a consensus supporting the recommended change; then
5. DHS will make updates to the MISA based on the PWG's decision and forward the updated Agreement to all Participants.

Annual Review:

This Agreement should be reviewed annually by Federal Information Sharing Participants. If any recommended updates are identified, the Participant shall follow processes documented above for *Administrative Updates* and/or *Changes Other Than Administrative*.

Five-Year Review:

If possible, approximately six months prior to the five-year termination point of this Agreement DHS should identify a subset of Federal Information Sharing Participants, to include representatives from the MISA signatories on Page 8 to form a Policy Working Group (PWG) to review this Agreement. The PWG will act as representation for all Participants. The PWG

should review and update this Agreement to meet current requirements. The five-year review should follow the *Changes Other Than Administrative* processes documented above.

Termination:

Federal Information Sharing Participants may withdraw without terminating the Agreement for the remaining Participants. All provisions regarding the handling and protection of information and data exchanged under this Agreement shall remain in effect as long as any Federal Information Sharing Participant, or its designated users, remains in possession of any such data, records, or information derived from another Participant.

This Agreement will terminate effective five years from the last day of the month of the first MISA signature, unless replaced sooner or agreed to be extended by the extant Federal Information Sharing Participants.

Supersession:

This Agreement supersedes the Enhance Shared Situational Awareness Multilateral Information Sharing Agreement, dated March 2015.

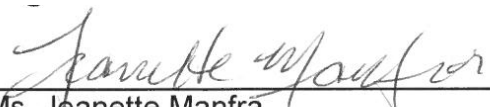
Accession:

This Agreement is open to accession by all Federal Departments and Agencies by signature of an authorized official, with a signed copy to be promptly deposited with the DHS. Reservations are not permitted.

Points of Contact:


The points of contact responsible for handling administrative activities related to this Agreement are DHS: cyberliaison@hq.dhs.gov.

Signatories:



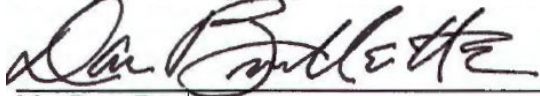
Ms. Jeanette Manfra
Assistant Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency

12/14/18
Date



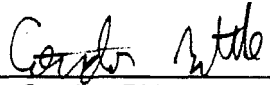
Ms. Essye B. Miller
Principal Deputy, DoD Chief Information Officer

31 Dec 18
Date



Mr. Dan Brouillette
Deputy Secretary, Department of Energy

FEB 08 2019
Date



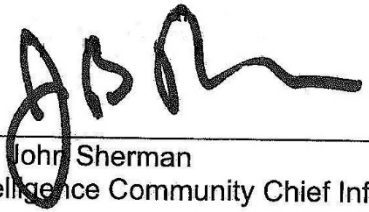
Mr. Gordon Bitko
Assistant Director and Chief Information Officer, Federal Bureau of Investigation

8-Feb-19
Date



Mr. George C. Barnes
Deputy Director, National Security Agency

12/21/18
Date



Mr. John Sherman
Intelligence Community Chief Information Officer, Office of the Director of National Intelligence

4 DEC 2018
Date



Vice Admiral Nancy A. Norton
Director, Defense Information Systems Agency

24 OCT 19
Date

ANNEX A: Cybersecurity Functions as Described by the Information Sharing Architecture (ISA)

| Functions | Functional Activities | Descriptions |
|---|---|--|
| Network Operations Function (NOF) | Infrastructure Operations/ Management | Routine network operations including network configuration, monitoring, and modification. |
| | Configuration Management | Software, hardware and firmware, Trust Chain Mapping, and validation of authenticity. |
| | Risk Identification, Management and Reduction | Identification and assessment of local risks including assessment of applicability and susceptibility, in light of information regarding current vulnerabilities and existing threat activity. |
| | Certification and Accreditation | Compliance with security governance and maintenance of records of said compliance. |
| Computer Network Defense Function (CNDF) | Detection and Mitigation | Frontline detection of anomalous behavior and implementation of pre-established mitigation techniques. |
| | Remediation | Activities to reestablish the trusted environment following incident response and mitigation. |
| | Focused Vulnerability Assessment | Assessment of applicability and susceptibility in light of information regarding vulnerabilities or existing threat activity. |
| Domain/ Sector Awareness Function (DSAF) | Status Aggregation and Reporting | Consolidation, filtering, and release of information regarding network operations, including detections, to external entities, allowing for the development of comprehensive enterprise awareness to support dissemination. |
| | Risk Assessment | Assessment of risk using internal and external information with an emphasis on risk to ability to achieve mission and operational objectives, as opposed to strict Information Technology (IT) vulnerability assessment. |
| | Information Validation and Dissemination | Collection, assessment for applicability and validity, and dissemination of information from external entities to other functions. |
| Threat Assessment Function (TAF) | Incident and Threat Discovery | Discovery or determination that a new event can be determined to adversary-based or intentional. |
| | Threat Characterization and Assessment | Analysis and assessment of adversary activity such that an evolving characterization of their abilities, reach, techniques, and intent are maintained and available across the community, which may involve fusion of available information from multiple sources. |

UNCLASSIFIED

| | | |
|--|---|---|
| | Forensics and Malware Analysis | Systematic analysis of threat activity, malware, or other related adversary artifacts. |
| | Development of Indicators and Warnings Based on Threat Assessment | Creation of indications and warnings to disseminate knowledge based on threat assessment. |
| | Mitigation and Signature Development | Development of static signatures, behavioral characterization, and other descriptors of threat activity derived from threat assessment that can be used for CNDF and NOF purposes and development of mitigation techniques, configurations, or processes based on analysis of threat activities, including pre-established mitigations. |
| Threat Operations Function (TOF) | Operations Planning, Coordination and Execution | Cyber-based operations applied to adversary capabilities. |
| | Characterization of Achievable Reach and Effects | Development of an evolving description of the mission effects achievable by our forces when applied to adversary capabilities. |
| | Damage and Consequence Assessment | Assessment of the specific or potential effectiveness of a threat activity. |
| Integrated Operational Action Planning Function (IOAPF) | Course of Action (COA) Development and Selection | Coordination and development of actions that can be executed within or across operational areas. COAs can also be automated to trigger on specified activities. |
| | Mitigation Planning | Development and dissemination of comprehensive mitigation plans (preemptive and responsive). |
| | Equities Assessment | Assessment across multiple areas of relative risk, mission impact, and achievable effects in determining which COA or mitigation actions are valid and appropriate. |
| Integrated Operational Action Coordination Function (IOACF) | Action Activation and Tracking | Active initiation of a particular mitigation and action plan and monitoring of its progress through execution. |
| | Integrated Coordination and Reporting | Exchange of information for the purposes of orchestration and coordination of inter-related steps. |
| | Effectiveness Assessment | Assessment of the relative success of an ongoing (or completed) action plan in meeting operational objectives. |

ANNEX B: Cybersecurity Enduring Functional Exchanges (EFE) as Defined by the Information Sharing Architecture (ISA)

| Information Exchanges | Description | Information Exchange Types |
|---|--|--|
| <p>EFE 1: Configuration/ Anomaly Reporting</p> | <p>Configuration/Anomaly Reporting includes information that describes the configuration and status of a network. This configuration information is critical in determining the risk exposure to vulnerability or a specific exploitation strategy. The status information includes the reporting of network behavior that is unusual but has not been characterized as malicious.</p> | <p>Risk Posture: Configuration-specific status of the relative exposure of a network to a specified vulnerability.</p> |
| | | <p>Anomalies: Events or alerts indicating unexpected network behavior or traffic.</p> |
| | | <p>Infrastructures: Detailed configuration or other network information that may be requested because of an active or projected exploit to determine risk to or posture of an enterprise; information necessary to determine applicability of vulnerability information.</p> |
| <p>EFE 2: Knowledge of Threat Actors</p> | <p>Knowledge of Threat Actors consists of the information and analysis products that are available to, and developed by, ISA Participants.</p> | <p>Threat Actor Infrastructure: Information specific to actor techniques, intent, means, and history.</p> |
| | | <p>Threat Actor Personas: Information that provides a correlation between actor intent and the capabilities of individual actors.</p> |
| | | <p>Threat Actor Attribution: Association of a specific activity to an entity. This can be based on specific exploits used and associated tradecraft.</p> |
| | | <p>Trend Analysis: Analysis and characterization of threats across domains, across specific spaces, or globally.</p> |
| | | <p>Victim Information: Information regarding potential or exploited victims of specific threat actors.</p> |
| | | <p>Threat Actor Indicators: Indicators specific to a threat actor (Signatures are descriptors of threat activity that are characterized so they can be used as mechanisms to monitor, detect, or intercept future instances of the same events.)</p> |
| <p>EFE 3: Incident Awareness</p> | <p>Incident Awareness consists of exchanges that encompass information about "What Am I Seeing"?</p> | <p>Incident Information: Description and characterization of emerging and ongoing events and incidents; these specifics would be used to create alerts or warnings issued to peer organizations.</p> |

UNCLASSIFIED

| | | |
|---|--|---|
| | | <p>CNO Awareness: Awareness of current and planned CNO operations that would prevent the activity being characterized as malicious.</p> |
| | | <p>Incident Data: Data related to an incident that is shared for the purpose of analysis, mitigation or signature development (i.e., actual malware or Packet Capture File format files).</p> |
| | | <p>Infrastructure Impact/Effects: Impacts and effects of the incident on the infrastructure.</p> |
| | | <p>Victim Information: Compromised entities associated with a specified incident.</p> |
| | | <p>Alerting Indicators: Descriptors of threat activity that can be characterized so they can be used as mechanisms to monitor or intercept future instances of the same events.</p> |
| <p>EFE 4: Indications & Warnings</p> | <p>Indications and Warnings are the information items that can provide time critical notification and alerting criteria.</p> | <p>Events and Alerts: NRT notifications that will spur actions or assessment at other partners. Tipping and cueing are a specialized form of alerting that is exchanged through dedicated information channels.</p> |
| | | <p>Warnings: Machine speed-level notifications that indicate a specific, emergent risk associated with a confirmed threat. Warnings would include flash-level notifications of detected events, threats, or findings of national significance, CRITICs.</p> |
| | | <p>Impact Assessments: Machine speed-level notifications that indicate the relative risk to operations as determined by a domain; may range from a general indicator of change in Cyber Condition (CYBERCON) to a more detailed indicator of mission achievability.</p> |
| | | <p>Potential Indicators: Descriptors of threat activity that can be characterized so they can be used as mechanisms to detect future instances of the same events.</p> |
| <p>EFE 5: Vulnerability Knowledge</p> | <p>Vulnerability Knowledge consists of the discovered vulnerabilities in software, hardware, and infrastructure components. This allows for the assessment of the exposure level of specific networks or organizations</p> | <p>Vulnerabilities: Technical design or implementation flaws in IT products or systems that permit exploitation or attack by an unauthorized party.</p> |
| | | <p>Exploits: Known intrusion and exploitation techniques or patterns (may or may not be directly correlated to vulnerabilities) that can be mitigated.</p> |

UNCLASSIFIED

| | | |
|--|---|---|
| | relative to a specific vulnerability. | Potential Victim Information: Information about entities that are of high risk to vulnerability or exploit. |
| EFE 6: Mitigation Strategies | Mitigation Strategies consist of the sets of actions that can be executed to reduce the impact or possibility of an intrusion or to a vulnerability exposure. | Coordinated Action Plans: Integrated action plans developed across multiple domains, including equities, dependencies, and sequencing. |
| | | Courses of Action: Preplanned and approved integrated action plans that can be configured on defensive systems for machine-speed execution. |
| | | Understanding of Achievable Mitigation Effects: Operational characterization of available capabilities. |
| EFE 7: Mitigation Actions and Responses | Mitigation Actions and Responses are specific steps that are used to reduce or prevent the impact of an intrusion or vulnerability | Tasking and Status: Tasking and confirmation messaging intended to communicate direction or status regarding action plan execution. |
| | | Computer Network Operations (CNO) Capability Awareness: Knowledge of possible CNO activities that can be employed to mitigate a threat. |
| | | Effectiveness Reporting: Communication of effectiveness of mitigation activities at the national, mission, or operational level (versus IT or CND configuration level, part of the IT Configuration EFE). |
| | | After-Action/Lessons Learned Information: Information regarding closure of action or effectiveness efforts. |

ANNEX C: MISA SIGNATORIES AS OF JUNE 2018

1. DHS - Department of Homeland Security
2. DOC - Department of Commerce
3. DOD - Department of Defense
4. DOE - Department of Energy
5. DOI - Department of Interior
6. DOJ/FBI - Department of Justice –FBI
7. DOJ - Department of Justice
8. DOL - Department of Labor
9. DOS - Department of State
10. DOT - Department of Transportation
11. EDU - Department of Education
12. EPA - Environmental Protection Agency
13. GSA - General Services Administration
14. HHS - Department of Health and Human Services
15. HUD - Department of Housing and Urban Development
16. NASA - National Aeronautics and Space Administration
17. NRC - Nuclear Regulatory Commission
18. NSF - National Science Foundation
19. OPM - Office of Personnel Management
20. SBA - Small Business Administration
21. SSA - Social Security Administration
22. TREAS - Department of Treasury
23. USAID - United States Agency for International Development
24. USDA - United States Department of Agriculture
25. VA - Department of Veterans Affairs
26. CFPB - Consumer Financial Protection Bureau
27. FDIC - Federal Deposit Insurance Corporation
28. OSHRC - Occupational Safety and Health Review Commission
29. PBGC - Pension Benefit Guaranty Corporation
30. SEC - U.S. Securities and Exchange Commission
31. TVA -- Tennessee Valley Authority
32. DC3 - Defense Cyber Crime Center
33. DISA - Defense Information Systems Agency
34. NSA - National Security Agency
35. ODNI - Office of the Director of National Intelligence
36. USCC - United States Cyber Command

ANNEX D: Acronyms

| | |
|----------|--|
| ACS | Access Control Specification |
| CISA | Cybersecurity Information Sharing Act of 2015 |
| CNDF | Computer Network Defense Function |
| CNO | Computer Network Operations |
| COA | Course Of Action |
| CYBERCON | Cyber Condition |
| DSAF | Domain/Sector Awareness Function |
| EFE | Enduring Functional Exchanges |
| EO | Executive Order |
| ESSA | Enhance Shared Situational Awareness |
| FICAM | Federal Identity, Credentials, and Access Management |
| IOACF | Integrated Operational Action Coordination Function |
| IOAPF | Integrated Operational Action Planning Function |
| IC-SCC | Intelligence Community-Security Coordination Center |
| IT | Information Technology |
| ISA | Information Sharing Architecture |
| MISA | Multilateral Information Sharing Agreement |
| NOF | Network Operations Function |
| NSC | National Security Council |
| OMB | Office of Management and Budget |
| PPD | Presidential Policy Directive |
| PWG | Policy Working Group |
| REF | Reference |
| SOC | Summary of Conclusions |
| TAF | Threat Assessment Function |
| TOF | Threat Operations Function |

ANNEX E: Track Changes Table

| <u>Version</u> | <u>Date (Final)</u> | <u>Page, Line</u> | <u>Changed Content</u> |
|----------------|---------------------|-------------------|--|
| 1.1 | 2016 | | None Available |
| 1.1a | 10/2019 | All Pages | Footer changed from "Version 1.1" to "Version 1.1a" |
| 1.1a | 10/2019 | 2, 67 | ", as applicable to particular sets of information." added |
| 1.1a | 10/2019 | 3, 87-88 | ", where the latter is specifically invoked with respect to a particular set of information." added |
| 1.1a | 10/2019 | 3, 110-111 | " to the extent that CISA is invoked with respect to a particular set of information" added |
| 1.1a | 10/2019 | 6, 274-277 | "When a change other than administrative is identified, DHS will identify a subset of Federal Information Sharing Participants, to include representatives from the MISA initial seven signatories on Page 8, to form a Policy Working Group (PWG) to review and consider recommended changes that are other than administrative." <ul style="list-style-type: none"> - "should" replaced by "will" - "initial seven" added |
| 1.1a | 10/2019 | 16, 356 | Annex E and corresponding tracking changes table added |