606-22

CYBERSECURITY GROUP

# RANGE COMMANDERS COUNCIL CYBERSECURITY GROUP GUIDEBOOK

**ABERDEEN TEST CENTER**
**DUGWAY PROVING GROUND**
**ELECTRONIC PROVING GROUND**
**REAGAN TEST SITE**
**REDSTONE TEST CENTER**
**WHITE SANDS TEST CENTER**
**YUMA PROVING GROUND**

**NAVAL AIR WARFARE CENTER AIRCRAFT DIVISION PATUXENT RIVER**
**NAVAL AIR WARFARE CENTER WEAPONS DIVISION CHINA LAKE**
**NAVAL AIR WARFARE CENTER WEAPONS DIVISION POINT MUGU**
**NAVAL SURFACE WARFARE CENTER DAHLGREN DIVISION**
**NAVAL UNDERSEA WARFARE CENTER DIVISION KEYPORT**
**NAVAL UNDERSEA WARFARE CENTER DIVISION NEWPORT**
**PACIFIC MISSILE RANGE FACILITY**

**96th TEST WING**
**412th TEST WING**
**ARNOLD ENGINEERING DEVELOPMENT COMPLEX**

**SPACE LAUNCH DELTA 30**
**SPACE LAUNCH DELTA 45**

**NATIONAL AERONAUTICS AND SPACE ADMINISTRATION**

This page intentionally left blank.

**606-22**

# RANGE COMMANDERS COUNCIL CYBERSECURITY GROUP GUIDEBOOK

**February 2022**

**Prepared by**

**CYBERSECURITY GROUP**

**Published by**

**Secretariat**
**Range Commanders Council**
**US Army White Sands Missile Range**
**New Mexico 88002-5110**

This page intentionally left blank.

# Table of Contents

This page intentionally left blank.

# Preface

This product is the result of a task to create a cybersecurity range systems interconnection agreement standard. Interconnection documentation is not currently standardized, which often makes creating such documentation more time-consuming than necessary. In addition, the document is designed to assist the ranges in reducing the language gap in terminology that exists between Services due to the way the Risk Management Framework has been implemented. All Range Commanders Council member ranges would benefit from the use of standardized templates and guidelines.

For information about this document, please contact the RCC Secretariat office.

Secretariat, Range Commanders Council
ATTN: TEWS-TDR
1510 Headquarters Avenue
White Sands Missile Range, New Mexico 88002-5110
Telephone:(575) 678-1107, DSN 258-1107
E-mail: rcc-feedback@trmc.osd.mil

This page intentionally left blank.

# Acronyms

| | |
|---|---|
| AO | authorizing official |
| CIO | chief information officer |
| CISO | chief information security officer |
| CTO | chief technology officer |
| ISA | Interconnection Security Agreement |
| ISSM | information security manager |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |

This page intentionally left blank.

# 1. Scope

This document provides guidance and documentation requirements concerning the templates provided by the Range Commanders Council (RCC).

# 2. Purpose

This document provides a standardized resource for different agencies and test ranges in order to support reciprocity and interconnectivity through the development of artifacts.

# 3. Reciprocity Definitions

Definitions common to all RCC CSG groups can be found in the RCC CSG Lexicon.[1] Definitions specific to this document are located below.

a. Party A – Tenant. (Example: Resource Consumer/Requestor) Author/Initiator

b. Party B – Host. (Example: Resource Provider) Contributor/Evaluator

c. Authorizer or Designee. Person authorized to sign documentation on behalf of the party. (Examples: Authorizing Official Designated Representative, Functional Authorizing Official, Designated Authorizing Official, Chief Information Officer [CIO], Chief Technology Officer [CTO], Chief Information Security Officer [CISO], Information System Security Manager [ISSM], Program Manager, Program Executive Officer)

# 4. Template Usage

The following are required formatting styles to be used in preparing cybersecurity documents. The RCC Document Template and Formatting Guide[2] provides further information. If you find something wrong with this template, please contact the RCC Secretariat.

a. Black in braces – items requiring input/edit by document author.

b. Blue in brackets – guidance for the section to be filled out.

c. One space between a period and the start of a new sentence.

d. Ensure spacing between paragraphs.

# 5. Documentation Selection Guidance

This section provides a means for the user to determine which documents may be needed for interconnections. This guidebook attempts to address common scenarios for interconnection situations involving authorizing officials (AOs) or equivalent. However, all situations may not have been addressed. It is incumbent upon the parties to negotiate the artifacts needed to facilitate the connection.

---

[1] Range Commanders Council. *Cybersecurity Lexicon*. 605-21. April 2021. May be superseded by update. Retrieved 24 August 2021. Available to RCC members with private page access at https://www.trmc.osd.mil/wiki/x/sYc4Bg.

[2] Range Commanders Council. *RCC Document Template and Formatting Guide*. January 2021. May be superseded by update. Retrieved 24 August 2021. Available to RCC members with private page access at https://www.trmc.osd.mil/wiki/download/attachments/78348636/Desk%20Reference%20-%20RCC%20Document%20Template%20and%20Formatting%20Guide.pdf.

### 5.1 Same AO

When the connections to be made involve systems authorized by the same AO, typically the only document needed is an Interconnection Security Agreement (ISA). Optionally, a Memorandum of Understanding (MOU) may be desired.

### 5.2 Different AOs

When the connections to be made involve systems authorized by different AOs, typically an MOU and ISA are needed to document the connection.

### 5.3 No AO to AO

When there is only a single party with an AO, both parties will need to work together to determine the documentation needed. Sometimes an MOU and ISA can be completed to satisfy the needs of the parties but it may be necessary to seek legal guidance. All of these situations should be evaluated on a case-by-case basis.

### 5.4 No AOs

The parties participating in this connection will need to make their own determination as to what documentation will be needed to identify and record the connections and satisfy both parties' requirements. (Example: customer using range space without connectivity.)

### 5.5 Common Supporting Artifacts

This list of artifacts is not to be considered all-inclusive but as a listing of common supporting artifacts that may be requested to support an interconnection.

a. MOU
b. ISA
c. Range specific approval documentation
d. Spectrum Management Coordination/Approval
e. Authorization/Accreditation Letter
f. Port Scan
g. Vulnerability Scan
h. Security controls (Risk Management Framework Access)
i. Security Assessment Report
j. Risk Assessment/Report
k. Plan of Actions and Milestones

## 6. Documentation

### 6.1 Memorandum of Understanding

The MOU documents a general understanding between two parties represented by AOs or designees to approve interconnection of information systems while considering residual risk

and impact. An MOU is put into place for matters where the understanding does not involve reimbursement. Conversely, a Memorandum of Agreement (MOA) is put into place for matters where the agreement is expected to involve reimbursement or a commitment of resources. For more information concerning the use and format of an MOA refer to DoD Instruction 4000.19.[3] A template MOU is available here.

### 6.1.1 Document Structure and Examples

a. Background. In most cases, there is no need to discuss the background or provide justification, particularly if between DoD components. Occasionally, however, there is a desire to explain the need for the document; particularly where it is not self-evident from the Purpose or it is with a federal agency.

b. Authorities. There may be no need to include items in this section. If included, it should contain a list of documents that provide governance for the parties.

c. References. This section should list references utilized in the creation of the MOU.

d. Purpose. This section must contain a succinct statement about the intention of the MOU.

e. Understanding of the Parties. This section must describe the intentions/responsibilities of each party.

f. Personnel. This section must detail that the MOU does not change how personnel associated with the MOU are compensated. Funding does not cross boundaries between host and tenant in regards to an MOU.

g. General Provisions. This section covers all generalities of the MOU. The elements in this section are required and may contain required verbiage that is not to be altered and is indicated as mandatory content in the MOU template.

   (1) Points of Contact. This section must identify the points of contact for the parties.

   (2) Correspondence. This section must identify explicit actions to be taken regarding correspondence between parties concerning the MOU.

   (3) Funds and Manpower. This section must state that an MOU does not document or provide for the exchange of funds or manpower between the parties nor does it make any commitment of funds or resources.

   (4) Modification of MOU. This section must identify the acceptable methods to modify the MOU.

   (5) Disputes. This section must identify the legal guidance for dispute handling concerning the MOU.

   (6) Termination of Understanding. This section must identify that both parties have equal capability to terminate the MOU.

   (7) Transferability. This section must identify that all parties of the MOU must consent in writing to transfer the MOU's applicability.

[3] Department of Defense. *Support Agreements*. DoDI 4000.19. 16 December 2020. May be superseded by update. Retrieved 24 August 2021. Available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/400019p.pdf.

(8) Entire Understanding. This section must state that the MOU details the complete understanding of party involvement.

(9) Effective Date. This MOU takes effect beginning on the day after the last party signs.

(10) Expiration Date. This section must identify the date representing when the applicability of the MOU is dissolved. An MOU is not open-ended and the duration typically does not exceed three years. The length of the understanding can exceed three years but this should be determined by the appropriate authorities.

(11) Cancelation of Previous MOU. This section must identify what MOUs may be superseded by the current MOU. Complete this section only when superseding a previous MOU.

h. Enclosures. This section must list any supporting documentation to accompany the MOU.

i. Approved. This section shows the understanding between parties has been approved by the signatures of the AOs or designees. Signatures should never be alone on a separate page.

### 6.1.2 MOU Signatures

a. Recommended. Signature authority for the MOU is the responsibility of the representative AO. The AO may also designate signature authority for systems that allows them to take responsibility for the connection and its risks; thus their signature should be considered sufficient for systems within their oversight. (Examples: AO or AO Designee)

b. Alternate. When there is no AO or AO designee, other personnel fulfilling the role of an AO may be required to sign the documentation. The key to choosing a signature authority for the documentation is to make sure they had the management of resources and the authority to commit within their duty scope. (Examples: CIO, CTO, CISO, Program Manager, Program Executive Officer, or other AO equivalent.)

### 6.1.3 MOU Routing and Staffing Recommendations

The authoring party will route the unsigned draft to the other party(s) for review and concurrence. Once all parties concur with the draft, the authoring party will sign the document and route it to the other parties for signature. Each party should use existing internal routing processes. Recommended reviewers may include: contracts, budget, information technology, security, legal, and administrative.

## 6.2 Interconnection Security Agreement

The ISA documents the technical implementation of the specific connections between parties. An ISA is commonly used for specific events, repetitive/recurring events, or cyclic events. An ISA's effectivity is bound by a specific duration with options for extension during approved situations. If an MOU is associated with this ISA, the dates of the ISA extension must be within scope of the MOU. Interconnection architecture changes must be coordinated between parties to determine whether a new ISA must be signed/renewed. A template ISA is available here.

### 6.2.1 **Document Structure and Examples**

#### 6.2.1.1 Interconnection Statement of Requirements

This section should include a general statement of what connection is required and why. The ISA is not a promise/agreement of resources. If a commitment of resources is required, it should be handled within an MOA.

[Example: The requirements for interconnection between Party A and Party B are for the express purpose of exchanging data between System A, owned by Party A, and System B, owned by Party B. Party B requires the use of Party A's (database name) and Party A requires the use of Party B's (database name), as approved and directed by the Secretary of (Agency Name) in (Proclamation name) dated (date). The expected benefit is to expedite the processing of data associated with (Project name) within prescribed timelines.]

#### 6.2.1.2 System Security Considerations

a. General Information/Data Description/Types. This section must describe the connection in layman's terms, to include the purpose of the data traversing the boundary and how the connection is made.

   [Example: The interconnection between System A, owned by Party A, and System B, owned by Party B, is a two-way path. The purposes of the interconnection are to deliver the XYZ database to Party B's Data Analysis Department and to deliver the ABC database to Party A's Research Office.]

b. Description and Diagram of Data Flow. This section must include a detailed description of the data flow and should be easily recognizable when comparing with the network topology/data-flow diagram(s). It must address the direction of data flow as well as the purpose, source, and destination. Based upon complexity, it may be beneficial to have separate data flow and topology diagrams.

c. Ports, Protocols, and Services (PPS) Offered. This section must include a table logging the ports and protocols required to traverse the interconnection boundary and the services operating on the connection. Table 1 shows an example PPS table.

**Table 1. Example Ports, Protocols, and Services Table**

| Network | SOURCE PORT | DESTINATION PORT | Protocol | Service |
|---|---|---|---|---|
| **(Authority to Operate [ATO] Network Name)** | **443** | **49000** | **https** | **Secure web** |
| | | | | |
| | | | | |

d. Data Sensitivity/Criticality. This section must include the sensitivity and criticality of data exchanged between the parties. This is tailored to the security categorization requirements for the data traversing the interconnection requested. Describe the sensitivity level of the information that will be handled through the interconnection, including the highest level of sensitivity involved (e.g., Privacy Act, Trade Secret Act, Law Enforcement Sensitive, Sensitive-But-Unclassified) and the most restrictive

protection measures required. Table 2 shows an example Data Sensitivity/Criticality table.

**Table 2. Example Data Sensitivity/Criticality Table**

| | |
|---|---|
| Classification | TS/S/U |
| Caveats | SCI/SAP |
| Dissemination | CUI/NOFORN/PII/PHI |
| CIA of Network | Ex: M-L-L |
| | |
| **Data Type** | **CIA Impact** |
| Ex: TSPI | Ex: L-L-L |
| Data Type 2 | CIA Impact |
| Data Type 3 | CIA Impact |

e. General User Roles and Responsibilities. This section must include the following descriptions: the roles and responsibilities of general users with access to the data or systems between the parties; and personnel security requirements and responsibilities. General users do not normally have the ability to change security configurations on the connecting systems. System user responsibilities include, but are not limited to, adhering to organizational policies that govern acceptable use of organizational systems; using the organization-provided information technology resources for defined purposes only; and reporting anomalous or suspicious system behavior.[4]

   [Example: "All Party A general users with access to the data received from Party B are U.S. citizens with a valid and current Party A background investigation. All Party B general users with access to the data received from Party A are U.S. citizens with a valid and current Party B background investigation."]

f. Privileged User Roles and Responsibilities. This section must include a description of the roles and responsibilities of privileged users and describe expectations for data/system protection. System administrator responsibilities may include, but are not limited to, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup, recovery, and reconstitution activities; implementing controls; and adhering to and enforcing organizational security and privacy policies and procedures. (NIST SP 800-37 Rev 2)

   [Example: "In addition to the general user requirements, privileged users must fulfill all party elevated privileged requirements."]

g. Information Exchange Security. This section must address the security measures in place at the boundary connection. Examples include access control lists, virtual local area network, and encryption.

[4] National Institute of Standards and Technology. *Risk Management Framework for Information Systems and Organizations*. SP 800-37 Rev 2. December 2018. May be superseded by update. Retrieved 24 August 2021. Available at https://doi.org/10.6028/NIST.SP.800-37r2.

[Example: "The security of the information being passed on this two-way connection is protected through the use of FIPS 140-2[5] approved encryption mechanisms. Individual users will not have access to the data except through their systems security software inherent to the operating system. All access is controlled by authentication methods to validate the approved users."]

h. Physical Security. This section must describe the physical security controls associated with the connection.

[Example: "The connections at each end are located within controlled access facilities, Open Storage Areas, or guarded 24 hours a day."]

i. Incident Response and Reporting. This section must describe the incident handling and reporting requirements for each party. In addition, the party discovering a security incident will notify the other party per the terms of the agreement.

[Example: "The party discovering a security incident will report it in accordance with its incident reporting procedures. In the case of Party B, any security incident will be reported to the Computer Security Incident Response Capability located at the Data Security Complex. Policy governing the reporting of security incidents is CC-2234."]

j. Audit Trail Responsibilities. This section must describe the auditing responsibilities and techniques for both parties. Common audit log information for collection is identified in Subsection 7.1.

[Example: "Both parties are responsible for auditing application processes and user activities involving the interconnection. Activities that will be recorded include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for one (1) year."]

k. System Maintenance Window. This section must describe the timeframes in which systems must have maintenance completed during the connection and any mitigations required.

[Example: "Maintenance may include but is not limited to any changes to the baseline such as STIGs or patching, will be performed on all systems every 60 days." "No maintenance will be required to be performed during the time of this agreement."

#### 6.2.1.3 Diagrams

This section must contain network, connectivity, and data flow diagrams in PDF, JPG, or similar format that depicts the interconnection. Use of a high-resolution image is preferred to allow detailed inspection of the connections. These may be separate diagrams depending on the complexity of the interconnection. An example diagram is provided in Figure 1.

[5] National Institute of Standards and Technology. *Security Requirements for Cryptographic Modules*. FIPS 140-2. 25 May 2001. May be superseded by update. Retrieved 24 August 2021. Available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

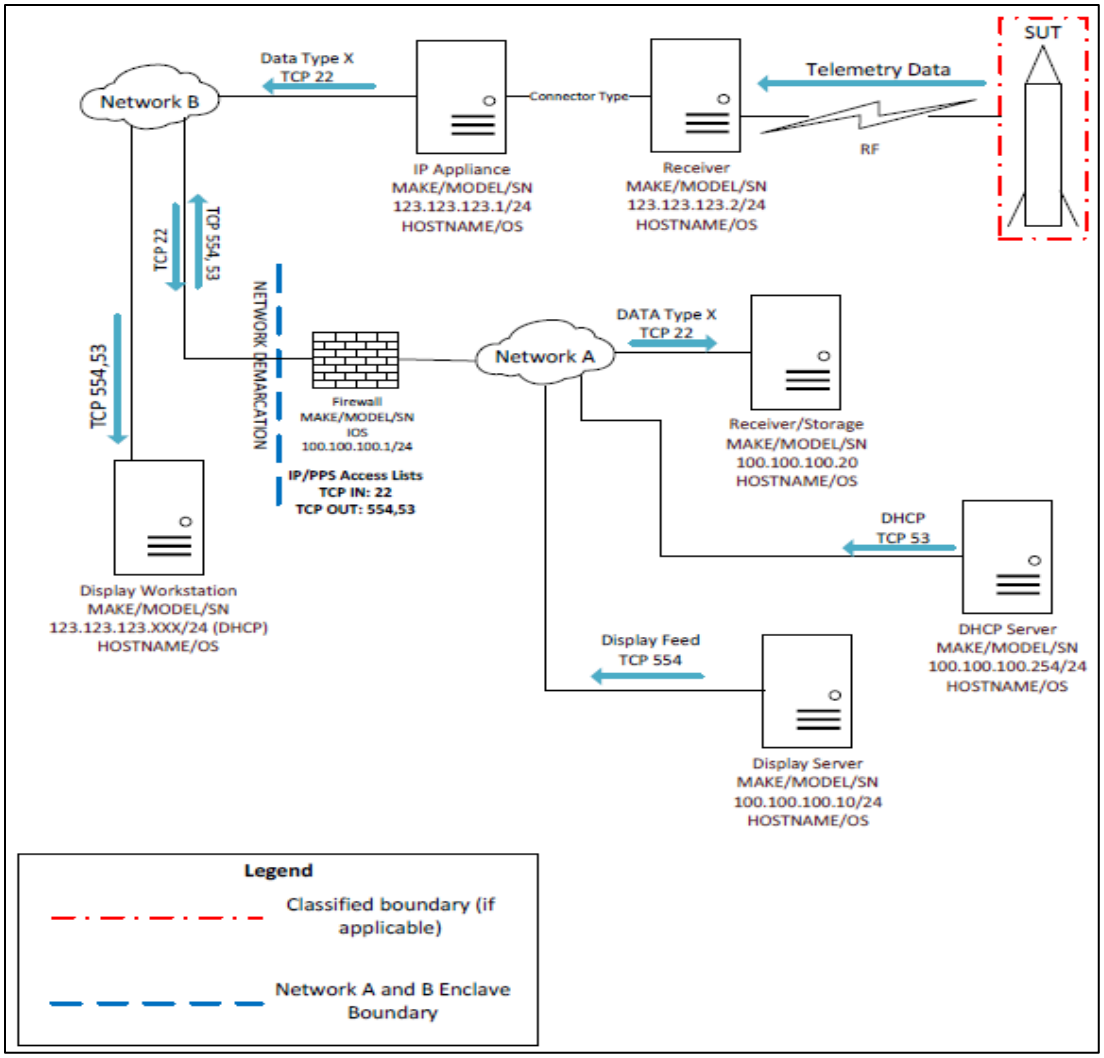


Figure 1. Example Network/Connectivity/Data Flow Diagram

#### 6.2.1.4 Test Dates and Duration

This section must describe the event(s) the ISA covers, to include dates and duration. If there is an MOU governing this connection the dates of the ISA must fall within the approved dates of the MOU.

#### 6.2.1.5 Appendixes

a. Appendix A: References. A list of all references the ISA derives information from.

b. Appendix B: Acronyms. A list of all connection-specific acronyms used within the ISA

c. Appendix C: Points of contact. A table is provided in the template to notate the key POCs for the ISA. Table 3 provides example points of contact tables.

**Table 3. Example Points of Contact Tables**

| **Party A** | | | |
|---|---|---|---|
| **Name** | **Title** | **Office Phone** | **Email** |
| | ISSM | | |
| | Network Engineer | | |
| | System Administrator | | |
| | Signing Party A | | |
| | Physical Security | | |
| | COMSEC Officer | | |
| | | | |
| **Party B** | | | |
| Name | Title | Office Phone | Email |
| | ISSM | | |
| | Network Engineer | | |
| | System Administrator | | |
| | Signing Party B | | |
| | Physical Security | | |
| | COMSEC Officer | | |
| | | | |

d. Appendix D: Hardware and Software Lists*. Separate tables are provided in the template to notate the critical information concerning hardware and software for each party covered in the ISA. Table 4 contains an example hardware and software table.

**Table 4. Example Hardware and Software Table**

| **Party A Hardware: List** | | | | |
|---|---|---|---|---|
| **Function** | **Hostname** | **Vendor** | **Model** | **Serial Number** |
| Data Server | {hostname1} | {Dell} | {PowerEdge} | AABBCC123 |
| Display Workstation | {hostname2} | {Dell} | {OptiPlex} | XXYYZZ123 |
| **Party A: Software List** | | | | |
| **Function** | **Vendor** | **Name** | **Version** | **Platform** |
| Network monitoring | Wireshark | Wireshark | 1.1 | Windows |
| **Party B: Hardware List** | | | | |
| **Function** | **Hostname** | **Vendor** | **Model** | **Serial Number** |
| Data Server | {hostname1} | {Dell} | {PowerEdge} | AABBCC123 |
| Display Workstation | {hostname2} | {Dell} | {OptiPlex} | XXYYZZ123 |
| **Party B: Software List** | | | | |
| **Function** | **Vendor** | **Name** | **Version** | **Platform** |
| Network monitoring | Wireshark | Wireshark | 1.1 | Windows |

e. Appendix E: Authority to Operate (ATO)/Authorization Decision Document*. Artifact showing approvals for the system that will have an interconnection for which the ISA is drafted.

f. Appendix F: Configuration Management/Control Board Approval*

g. Appendix G: Memorandum of Understanding*. Bundling with the ISA allows for review of approved understanding between parties when necessary.

h. Appendix H: Security Assessment Summary Report*. These are the summary pages that describe the compliant and non-compliant controls.

i. Appendix I: ISA Extension Memorandum*. The signed extension memorandum should be attached in this appendix. Subsection 7.2 contains an example memorandum. If an MOU is associated with this ISA, the dates of the ISA extension must be within scope of the MOU.

Note: * denotes optional element

#### 6.2.2 ISA Processing

##### 6.2.2.1 ISA Signatures

a. Recommended. Signature authority for the ISA is the responsibility of the representative ISSM/CIO and/or Command concurrence. The Command may also designate signature authority for systems that allows them to take responsibility for the connection and its risks; thus their signature should be considered sufficient for systems within their oversight.

b. Alternate. When there is no ISSM/CIO or Command concurrence other personnel may be required to sign the required documentation. The key to choosing a signatory for the documentation is to make sure they had the management of resources and the authority to commit within their duty scope. (Example: Non-DoD - CIO, CTO, CISO or other ISSM equivalent.)

#### 6.2.3 ISA Routing and Staffing Recommendations

The authoring party will route the unsigned draft to the other party(s) for review and concurrence. Once all parties concur with the draft, the authoring party will sign the document and route it to the other parties for signature. Each party should use existing internal routing processes. Recommended reviewers may include: information technology, security, and administrative.

# 7. Example Items

## 7.1 Example Audit Log Information

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.[6]

1. Review audit log configuration files for the correct settings. If doing a web review, SQL, or network devices use the settings from the current DISA Security Technical Information Guide.

[6] National Institute of Standards and Technology. "Content of Audit Records." AU-3. In *Security and Privacy Controls for Federal Information Systems and Organizations*. SP 800.53 Rev.4. 22 January 2015. Superseded by SP 800.53 Rev 5. Available here.

2. Review audit log configuration for Operating System. OS Audit Record configuration include:
   a) User ID
   b) Successful and unsuccessful attempts to access security files
   c) Date and time of the event
   d) Type of event
   e) Success or failure of event
   f) Successful and unsuccessful logons
   g) Denial of access resulting from excessive number of logon attempts (i.e. Account locked out)
   h) Blocking or blacklisting a user ID, terminal or access port, and the reason for the action
   i) Activities that might modify, bypass, or negate safeguards controlled by the system
   j) Data required to audit the possible use of covert channel mechanisms
   k) Privileged activities and other system-level access
   l) Starting and ending time for access to the system
   m) Security relevant actions associated with periods processing or the changing of security labels or categories of information

## 7.2 Example Memorandum for Record

{OFFICE SYMBOL} {DATE}

MEMORANDUM FOR RECORD

SUBJECT: {EXTENSION OF INTERCONNECTION SECURITY AGREEMENT}

1. {RATIONALE/JUSTIFICATION FOR EXTENSION OF THE ORIGINAL ISA}

2. {STATEMENT THAT THE ISA WAS REVIEWED AND DOES NOT NEED TO BE RENEWED}

3. {DATES THE ISA WILL BE EXTENDED TO}

4. The points of contact are: {POINTS OF CONTACT}

| | |
|---|---|
| {NAME} | {NAME} |
| {TITLE} | {TITLE} |
| {PARTY A} | {PARTY B} |

This page intentionally left blank.

# APPENDIX A

## Citations

Department of Defense. *Support Agreements*. DoDI 4000.19. 16 December 2020. May be superseded by update. Retrieved 24 August 2021. Available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/400019p.pdf.

National Institute of Standards and Technology. *Risk Management Framework for Information Systems and Organizations*. SP 800-37 Rev 2. December 2018. May be superseded by update. Retrieved 24 August 2021. Available at https://doi.org/10.6028/NIST.SP.800-37r2.

———. "Content of Audit Records." AU-3. In *Security and Privacy Controls for Federal Information Systems and Organizations*. SP 800.53 Rev.4. 22 January 2015. Superseded by SP 800.53 Rev 5. Available here.

———. *Security Requirements for Cryptographic Modules*. FIPS 140-2. 25 May 2001. May be superseded by update. Retrieved 24 August 2021. Available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

Range Commanders Council. *Cybersecurity Lexicon*. 605-21. April 2021. May be superseded by update. Retrieved 24 August 2021. Available to RCC members with private page access at https://www.trmc.osd.mil/wiki/x/sYc4Bg.

———. *RCC Document Template and Formatting Guide*. January 2021. May be superseded by update. Retrieved 24 August 2021. Available to RCC members with private page access at https://www.trmc.osd.mil/wiki/download/attachments/78348636/Desk%20Reference%20-%20RCC%20Document%20Template%20and%20Formatting%20Guide.pdf.

*** * * END OF DOCUMENT * * ***