<Insert Company Logo>

<Insert Company Name>

**Security Assessment Report,**

**System Security Plan, and**

**Plan of Action**

|  |  |
| --- | --- |
| Dated: <Insert Date> | <Insert First-name Middle-Initial Last-name>  <Title>  <Company Name>  <Company Address Line 1>  <Company Address Line 2>  <Phone Number>  <Email> |

This document includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this document. If, however, a contract is awarded to this offeror as a result of—or in connection with—the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government’s right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets <insert numbers or other identification of sheets>.

**Table of Contents**

[**1.0. Disclaimer** 3](#_Toc501108968)

[**2.0. About GTPAC** 4](#_Toc501108969)

[**3.0. Introduction and Overview** 5](#_Toc501108970)

[**3.1. About this Template** 5](#_Toc501108971)

[**3.2. Intended Audience** 8](#_Toc501108972)

[**3.3. Instructions on How to Utilize This Template** 9](#_Toc501108973)

[**3.4. How Security Control Compliance Information will be Documented and Organized** 12](#_Toc501108974)

[**4.0. Security Assessment Report, System Security Plan, and Plan of Action** 15](#_Toc501108975)

[**4.1. Company Profile** 15](#_Toc501108976)

[**4.2. General Overview of the System** 16](#_Toc501108977)

[**4.3. Security Control Compliance and Implementation Information** 18](#_Toc501108978)

# **1.0. Disclaimer**

This template was created by the Georgia Tech Procurement Assistance Center (“GTPAC”) and was funded through a cooperative agreement with the Defense Logistics Agency (“DLA”). This template is intended to be used in conjunction with the National Institute of Standards and Technology (“NIST”) Manufacturing Extension Partnership (“MEP”) Cybersecurity Self-Assessment Handbook (the “Handbook”), available at:

<http://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf>

This template is provided as a guide only, and the Georgia Institute of Technology, the Georgia Tech Research Institute, and GTPAC (collectively “Georgia Tech”) does not make any warranty, representation, or guarantee, either expressed or implied, with respect to the accuracy, completeness, or usefulness of this document and the information contained herein. Georgia Tech also makes no claims that use of this template will satisfy the regulatory requirements of the Department of Defense (“DoD”), Defense Federal Acquisition Regulation Supplement clauses 252.204-7008 and 252.204-7012 or the requirements outlined in NIST Special Publication 800-171 Revision 1. Compliance with these requirements can only be achieved through the proper implementation of the required security controls and policies and by adequately documenting a System Security Plan and Plan of Action.

It is our hope that providing this template will make the process of achieving compliance with DoD cybersecurity requirements easier for DoD government contractors. However, it is ultimately up to the contractor to assess its information technology systems and to assure that its implementation of the aforementioned controls, policies and documentation are adequate and meet all legal and regulatory requirements. By using this template, the contractor agrees that Georgia Tech is not responsible for any liabilities or damages that may result from the use of this template or the use of any processes or methods described herein. This template does not reflect the official views or policies of Georgia Tech or the DoD.

Issue Date: December 2017

# **2.0. About GTPAC**

GTPAC is a Procurement Technical Assistance Center (“PTAC”) that helps businesses identify, compete for, and win governments. For the past 31 years, the Defense Logistics Agency (“DLA”) has teamed with Georgia Tech to provide assistance to Georgia businesses navigating government contracting. GTPAC’s no-cost assistance to Georgia businesses comes in the forms of teaching, mentoring and coaching. GTPAC regularly offers free training seminars in-person and via webinar covering a whole range of government contracting topics. GTPAC is part of a nationwide network of PTACs which can be located at: [www.aptac-us.org](http://www.aptac-us.org).

# **3.0. Introduction and Overview**

# ***3.1. About this Template***

This template was produced by GTPAC in response to the Defense Federal Acquisition Regulation Supplement (“DFARS”) clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting,” which requires certain defense contractors with a covered contractor information system[[1]](#footnote-1) that processes, stores, or transmits covered defense information[[2]](#footnote-2) to immediately implement the cybersecurity controls outlined in NIST Special Publication (“SP”) 800-171[[3]](#footnote-3) (hereinafter “NIST SP 800-171”). NIST SP 800-171 provides a single set of performance-based security requirements for protecting “covered defense information” on “covered contractor information systems.” DFARS 252.204-7012, which is now being incorporated by in full-text or by reference in most DoD contracts, requires defense contractors to “implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.” *See* 252.204-7012(b)(2)(ii)(A).

Likewise, companion DFARS clause 252.204-7008, “Compliance with Safeguarding Covered Defense Information Controls,” requires defense contractors submitting an offer in response to most DoD opportunities to represent “that it will implement the security requirements specified by [NIST SP 800-171] … not later than December 31, 2017.” *See* DFARS 252.204-7008.

In December 2016, NIST issued a revision to NIST SP 800-171, called “Revision 1.” The revision outlined that NIST SP 800-171 requires that covered contractors create a “system security plan” and “plans of action” to achieve compliance. It states as follows:

Nonfederal organizations should describe in a system security plan, how the specified security requirements are met or how organizations plan to meet the requirements. The plan describes the system boundary; the operational environment; how the security requirements are implemented; and the relationships with or connections to other systems. Nonfederal organizations should develop plans of action that **describe how any unimplemented *security requirements will be met and how any planned mitigations will be implemented***. **Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.**

NIST SP 800-171, Rev. 1 at 9 (emphasis added).

On September 19, 2017, DoD issued a memorandum entitled “Implementation of DFARS Clause 252.204-7012,” which provides guidance to DoD acquisition professionals. The guidance acknowledged that a contractor could meet the contractual obligations to comply with NIST SP 800-171 by either fully implementing the security requirements outlined in NIST SP 800-171 Revision 1 and documenting such full implementation in its System Security Plan / Plan of Action, OR by implementing all the NIST SP 800-171 Revision 1 security requirements it could and carefully documenting in the contractor’s System Security Plan and Plan of Action, what requirements were implemented, how any unimplemented security requirements would be met, and how any planned mitigations would be implemented:

To document implementation of the NIST SP 800-171 security requirements by the December 31, 2017 implementation deadline, companies should have a system security plan in place, ***in addition to any associated plans of action to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems***.

“Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting,” by Shay D. Assad, Director, Defense Pricing/Defense Procurement and Acquisition Policy, dated Sept. 21, 2017, at pg. 3, available at: <https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf> (hereinafter “Assad memorandum”)

As noted above, there is no required format for a System Security Plan or Plan of Action, and they may be created as separate or combined documents.

The goal of this template is to provide government contractors with a **single combined document** that can used in conjunction with NIST’s Self-Assessment Handbook to: (1) document compliance with the 110 security requirements outlined in NIST SP-800-171 (e.g. create a “Security Assessment Report”), and to, (2) create a “System Security Plan” and “Plan of Action” which specifies how the NIST SP 800-171 security requirements are implemented, how and when any unimplemented security requirements will be met; how any planned mitigations will be implemented; and how and when the contractor will correct deficiencies and reduce or eliminate vulnerabilities. By completing this template in conjunction with NIST’s Self-Assessment Handbook, defense contractors will create a combination Security Assessment Report, System Security Plan and Plan of Action in a single document that can be used to establish compliance with NIST 800-171 Revision 1.

If the template is fully completed and properly filled out, contractors may have a document that establishes compliance with the above-mentioned cybersecurity related DFARS requirements.

As outlined in this template’s Disclaimer, GTPAC makes no claims that use of this template will absolutely ensure compliance with or satisfy the regulatory requirements of the DoD, the associated DFARS clauses mentioned above, or the security requirements outlined in NIST SP 800-171 Revision 1. Compliance with these requirements can only be achieved through the proper implementation of the required security requirements and policies and by drafting an adequate System Security Plan and Plan of Action. Further, it should be understood by the contractor, that merely meeting the minimum requirements of NIST 800-171 Revision 1 may not be enough to satisfy the DoD or other federal agencies when they conduct a risk assessment or evaluation of the contractor’s security. The entire purpose of requiring a “System Security Plan” and “Plan of Action” is to provide DoD with information they can use to evaluate the overall risk posed by a current or potential DoD contractor. DoD has indicated that it may analyze “a company’s system security plan and associated plans of action to evaluate the overall risk introduced” by the contractor’s internal information system/network. (Assad Memorandum at 4.) Indeed, it is important that contractors, when filling out this template, provide as complete and detailed information as possible as this document, when filled out, could be requested by the DoD to evaluate risk as part of the source selection process. (Assad Memorandum at 4-5.)

GTPAC hopes that providing this template it will make the process of drafting a System Security Plan and Plan of Action easier. However, it is ultimately up to the contractor to ensure that its implementation of the aforementioned requirements, controls, policies and documentation are adequate and that all legal and regulatory requirements have been met. Georgia Tech is not responsible for any liabilities or damages that may result from the use of this template, and the contractor assumes the risk that the use of this template may not meet all legal and regulatory requirements related to cybersecurity.

# ***3.2. Intended Audience***

This document is designed to be used by those responsible for managing the security and compliance of covered contractor information systems, and those who supply products and services to the DoD who must ensure “adequate security” by implementing NIST SP 800-171 Revision 1. These individuals may include those with system development life cycle responsibilities (e.g. program managers, business owners, system designers, developers, system administrators, and engineers) and individuals with security or risk management oversight responsibilities (e.g. chief information officers, chief information security officers, information security managers). Other individuals who may find this document useful include compliance officers, auditors, assessors and independent security consultants who are hired by a government contractor to provide security compliance assistance.

This template mentions official DoD policies and regulations related to cybersecurity. Such mention is public domain and does not constitute any policy statement by GTPAC or the DoD. GTPAC does not make or set procurement policy and makes no claims that the use of this template will satisfy the regulatory requirements of the DoD. All matters relating to the DFARS should be directed to the DoD.

# ***3.3. Instructions on How to Utilize This Template***

This template is designed to be used in conjunction with the NIST MEP Cybersecurity Self-Assessment Handbook (the “Handbook”), which was developed and published by NIST MEP. While the intended audience of the Handbook is manufacturers, it can be utilized by any DoD government contractor for conducting an assessment of NIST SP 800-171 security requirements. The Handbook, can be downloaded in full at:

<http://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf>

The goal of this TEMPLATE is to assist defense contractors in documenting their compliance with NIST 800-171, and developing a System Security Plan and Plan of Action, which is required by DFARS clause 252.204-7012 to be in place by December 31, 2017.

After the Handbook and this Template have been downloaded, four steps must generally be taken by the defense contractor:

**Step 1: In the TEMPLATE, the contractor should fill out Section 4.1 below, the Company Profile portion**. This will provide some general information about the defense contractor, including the Contractor’s Name, Point of Contact, Address, Telephone, Fax, Email, and other general information about the Contractor and their line of business. The Contractor is free to provide additional information if they so desire.

**Step 2: In the TEMPLATE, the contractor should fill out the “General Overview of the System” portion at Section 4.2 below.** This provides basic System Security Plan information about the covered information system at issue and describes, as required by NIST SP 800-171 Revision 1: (1) the system boundary; (2) the operational environment; and (3) the relationship with or connections to other systems. While a System Security Plan should also including information regarding “how the security requirements are implemented,” we will provide this information later on when answering the “System Security Plan and Plan of Action Questions” in step 4.

**Step 3: The Contractor should use the NIST MEP Handbook to conduct an assessment of their covered contractor information system and document the results of their assessment for each control in Section 4.3 of the TEMPLATE below.** As noted above, the Handbook provides a step-by-step guide to assessing a defense contractor’s information system against the security requirements in NIST SP 800-171. Section 3.4 of the TEMPLATE provides information on how NIST 800-171 Revision 1 security control compliance will be documented and organized in the TEMPLATE in Section 4.3. While you will use the Handbook to conduct the assessment, the results of the assessment will be marked, recorded, and documented for each of the 110 controls in Section 4.3 for each requirement. Specifically, contractors will indicate in the TEMPLATE below regarding each requirement whether:

* Your company fully meets the security requirement (“**YES**”)
* Your company does not meet the security requirement (“**NO**”)
* Your company partially meets the security requirement (“**Partially**”)
* The security requirement does not apply to the company’s environment (“**Does Not Apply**”) or;
* The company has taken an alternative but equally effective approach to meeting the security requirement (“**Alternative Approach**”).

This documentation in the TEMPLATE regarding what requirements are met or not met is sometimes called a “Security Assessment Report,” as it includes information from assessors necessary to determine what security controls are implemented or not implemented. This documentation provides important information to company management and government officials regarding what NIST SP 800-171 controls are met, what controls are not met, and the systems overall cybersecurity risk. The results of a security assessment ultimately influences security control implementation, and the content of respective System Security Plans and Plans of Action.

**Step 4:** **Finally, in the TEMPLATE, either during the course of the assessment (or shortly thereafter),** **the Contractor must provide detailed answers to the “System Security Plan and Plan of Action Questions” for each security requirement listed in Section 4.3 below.** As noted earlier, NIST SP 800-171 Revision 1 requires that contractors describe in a System Security Plan “how the specified security requirements are met” and “how organizations plan to meet the requirements.” NIST SP 800-171 at pg. 9. Contractors are also required to develop “plans of action” that describe “how any unimplemented security requirements will be met and how any planned mitigations will be implemented.” NIST SP 800-171 at pg. 9. NIST 800-171 Revision 1 allows a System Security Plan and Plan of Action to be documented in a combined manner. NIST SP 800-171 at pg. 9.

We have designed the “System Security Plan and Plan of Action Questions” in Section 4.3 below to elicit from the Contractor this required information. Therefore, if the Contractor fully and precisely answers the questions for each security requirement, they may achieve compliance. In short, contractors should review each requirement listed in Section 4.3, and answer the “Security Plan and Plan of Action Questions” accordingly. By answering the questions and providing the required information for each requirement, contractors will be creating with their answers the required “System Security Plan” and “Plan of Action” needed to achieve compliance by December 31, 2017.

Once each of these four steps are complete, the result will be a **single universal document** that, if filled out comprehensively and correctly, may meet the NIST SP 800-171 Revision 1 requirements.

Specifically, a completely filled out Section 4.0 thru 4.3 of the Template will result in the creation of:

* A **Security Assessment Report** of what NIST 800-171 Revision 1 security controls have been implemented or met;
* A **System Security Plan** that details the system boundary, the operational environment, the relationships with or connections to other systems and how the security requirements are implemented or how the contractor plans to meet these requirements;

and;

* A **Plan of Action** that describes how any unimplemented security requirements will be met and how any planned mitigations will be implemented.

Ultimately, the completion of Section 4.0 thru 4.3 of the TEMPLATE using the four steps above should result in achieving NIST SP 800-171 Revision 1 compliance, even if the defense contractor has not necessarily implemented all of the 110 security requirements outlined in NIST SP 800-171 Revision 1.

While full implementation of the 110 security requirements outlined in NIST SP 800-171 Revision 1 may not be necessary so long the contractor has an adequate Section 4.0 thru 4.3 of the TEMPLATE filled out, contractors should be aware that NIST SP 800-171 compliance could become a competitive discriminator, especially when it comes to DoD projects involving sensitive information.

DoD has indicated that in the future, System Security Plans and Plans of Action may be evaluated, and even warned that federal agencies may consider them when determining whether it is advisable to pursue an agreement or contract with the contractor.

# ***3.4. How Security Control Compliance Information will be Documented and Organized***

In Section 4.3, below, which will be used to document security control compliance, information about each security control is organized as follows:

* **Security Control Header:** This section provides information regarding the security control families associated number and name.
* **Security Control Subfamily:** This section indicates whether the security control is a “Basic Security Requirement” or a “Derived Security Requirement.”
* **Security Control Requirement:** This section provides a detailed description of the security control requirement as stated in NIST SP 800-171 rev. 1.
* **Security Control Implementation Details:** This section provides a detailed description of how the security control requirement is implemented. This section states whether the security control has been met using the following answers:

|  |  |
| --- | --- |
| **Yes** | The company fully meets the security requirement. |
| **No** | The company DOES NOT meet the security requirement. |
| **Partially** | The company partially meets the security requirement. |
| **Does Not Apply** | The security requirement does not apply to the company’s environment. |
| **Alternative Approach** | The company has taken an alternative but equally effective approach to meeting the security requirement. |

* **How the Security Requirements are Implemented:** If the answer is *Yes*, a statement should be included which explains how the information system implements the requirement.
* **How Any Unimplemented Security Requirements Will Be Met:** If the answer is *No*, a statement should be included which explains why the security requirement is not met. A statement should also be included which fully describes how the unimplemented security requirements will be met; how any planned improvements will be implemented, and when the improvements will occur.
* **How Any Planned Mitigations Will be Implemented:** If the answer is *No* or *Partially*, a statement should be included that explains what steps will be taken to mitigate risks created by the failure to fully implement the control. Discussion can include an explanation of what alternative steps have been taken to lessen security risks associated with the failure to fully implement a security requirement.
* **How the Security Requirement is Partially Met:** If the answer is *Partially*, a statement should be included which explains why the security requirement is partially met. A statement should also be included which fully describes how and when the partially met security requirements will be fully met, how any planned improvements will be implemented, and when the improvements will occur.
* **Why the Security Requirement Does Not Apply:** If the answer is *Does Not Apply*, a statement should be included which explains why the security requirement does not apply to your operational environment.
* **The Alternative Approach that is Implemented:** If the answer is *Alternative Approach*, a statement should be included which fully describes the alternative approach and how it is equally effective. A statement should also be included that explains how the information system implements the alternative approach.

Security control compliance information is detailed in the following format:

|  |
| --- |
| ***Security Control Header*** |
| ***Security Control Subfamily (Basic or Derived Security Requirements)*** |
| ***Security Control Requirement:***  ***<Number of Security Control>*** *<Text of 800-171 Control Requirement>* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  PLEASE ADDRESS THE FOLLOWING AREAS (WHERE APPLICABLE) AND PROVIDE EXPLANATIONS ACCORDINGLY  **How the Security Requirements are Implemented:**  <If the answer is *Yes*, a statement should be included which explains how the information system implements the requirement.>  **How Any Unimplemented Security Requirements Will Be Met:**  <If the answer is *No*, a statement should be included which explains why the security requirement is not met. A statement should also be included which fully describes how the unimplemented security requirements will be met; how any planned improvements will be implemented and when the improvements will occur.>  **How Any Planned Mitigations Will Be Implemented:**  <If the answer is *No* or *Partially*, a statement should be included that explains what steps will be taken to mitigate risks created by the failure to fully implement the control. Discussion can include an explanation of what alternative steps have been taken to lessen security risks associated with the failure to fully implement a security requirement.>  **How the Security Requirement is Partially Met:**  <If the answer is *Partially*, a statement should be included which explains why the security requirement is partially met. A statement should also be included which fully describes how and when the partially met security requirements will be fully met, how any planned improvements will be implemented, and when the improvements will occur.>  **Why the Security Requirement Does Not Apply:**  <If the answer is *Does Not Apply*, a statement should be included which explains why the security requirement does not apply to your operational environment.>  **The Alternative Approach that is Implemented:**  <If the answer is *Alternative Approach*, a statement should be included which fully describes the alternative approach and how it is equally effective. A statement should also be included that explains how the information system implements the alternative approach.> |

# **4.0. Security Assessment Report, System Security Plan, and Plan of Action**

# ***4.1. Company Profile***

* <Company Name>
* Point of Contact: <Name>
* <Address>
* <Telephone>
* <Fax>
* <Email>
* CAGE: <Insert CAGE #>, DUNS: <Insert DUNS #>.
* NAICS Codes: <Insert NAICS Codes>.

# ***4.2. General Overview of the System***

**<**Insert System Name & Type> is currently categorized as <Insert operational status> and is a <Insert System Type>.

The <INSERT SYSTEM NAME & DESCRIPTION>. The following table illustrates the categories and devices supported by <INSERT SYSTEM NAME>:

Table 3. <INSERT SYSTEM NAME> Categories and Devices

|  |  |  |
| --- | --- | --- |
| Category | Description | Managing Division(s) |
| Software |  |  |
| Hardware |  |  |
| Supporting Devices |  |  |

<Insert any additional desired system descriptions>

This Security Assessment Report, System Security Plan, and Plan of Action was approved on <Insert Date> by <Insert Name(s)> and has been review by <Insert Name(s)>.

**System Personnel**

System personnel contacts include contact information for the system owner, the contractor’s system POC, and the assigned security officer.

System Owner

|  |  |  |  |
| --- | --- | --- | --- |
| **Name:** |  | **Address:** |  |
| **Title:** |  | **Phone Number:** |  |
| **Agency:** |  | **E-mail Address:** |  |

*System POC*

|  |  |  |  |
| --- | --- | --- | --- |
| **Name:** |  | **Address:** |  |
| **Title:** |  | **Phone Number:** |  |
| **Agency:** |  | **E-mail Address:** |  |

*Information Security Officer*

|  |  |  |  |
| --- | --- | --- | --- |
| **Name:** |  | **Address:** |  |
| **Title:** |  | **Phone Number:** |  |
| **Agency:** |  | **E-mail Address:** |  |

**System Boundary**

**<**Insert Description of the System’s Physical Boundaries>

<Insert System Diagram>

**The Operational Environment**

<Insert Synopsis of System Operational Environment>

<Insert System Name> List of Applications and Software Supported

Software Applications on <INSERT SYSTEM NAME>

|  |  |  |
| --- | --- | --- |
| Software Application | Version | Synopsis or Description |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

<Insert Summary of Hardware Supported and Number of Users>

<Insert Summary of Devices Supported, General Description of Technology and Any Processes>

**The Relationships with or Connections to Other Systems**

<Insert information describing the systems relationships with or connections to other systems, including any interconnections and information sharing between the system and other systems>

# ***4.3. Security Control Compliance and Implementation Information***

**CONTRACTOR COMPLIANCE WITH THE**

**NIST SP 800-171 REV. 1 SECURITY REQUIREMENTS:**

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.1*** *Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.2*** *Limit system access to the types of transactions and functions that authorized users are permitted to execute.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.3*** *Control the flow of CUI in accordance with approved authorizations.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.4*** *Separate the duties of individuals to reduce the risk of malevolent activity without collusion.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.5*** *Employ the principle of least privilege, including for specific security functions and privileged accounts.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.6*** *Use non-privileged accounts or roles when accessing nonsecurity functions.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.7*** *Prevent non-privileged users from executing privileged functions and audit the execution of such**functions.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.8*** *Limit unsuccessful logon attempts.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.9*** *Provide privacy and security notices consistent with applicable CUI rules.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.10*** *Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.11*** *Terminate (automatically) a user session after a defined condition.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.12*** *Monitor and control remote access sessions.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.13*** *Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.14*** *Route remote access via managed access control points.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.15*** *Authorize remote execution of privileged commands and remote access to security-relevant information.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.16*** *Authorize wireless access prior to allowing such connections.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.17*** *Protect wireless access using authentication and encryption.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.18*** *Control connection of mobile devices.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.19*** *Encrypt CUI on mobile devices and mobile computing platforms.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.20*** *Verify and control/limit connections to and use of external systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.21*** *Limit use of organizational portable storage devices on external systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.1 ACCESS CONTROL*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.1.22*** *Control CUI posted or processed on publicly accessible systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.2 AWARENESS AND TRAINING*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.2.1*** *Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.2 AWARENESS AND TRAINING*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.2.2*** *Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.2 AWARENESS AND TRAINING*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.2.3*** *Provide security awareness training on recognizing and reporting potential indicators of insider threat.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.3 AUDIT AND ACCOUNTABILITY*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.3.1*** *Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.3 AUDIT AND ACCOUNTABILITY*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.3.2*** *Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.3 AUDIT AND ACCOUNTABILITY*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.3.3*** *Review and update audited events.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.3 AUDIT AND ACCOUNTABILITY*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.3.4*** *Alert in the event of an audit process failure.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.3 AUDIT AND ACCOUNTABILITY*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.3.5*** *Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.3 AUDIT AND ACCOUNTABILITY*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.3.6*** *Provide audit reduction and report generation to support on-demand analysis and reporting.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.3 AUDIT AND ACCOUNTABILITY*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.3.7*** *Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.3 AUDIT AND ACCOUNTABILITY*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.3.8*** *Protect audit information and audit tools from unauthorized access, modification, and deletion.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.3 AUDIT AND ACCOUNTABILITY*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.3.9*** *Limit management of audit functionality to a subset of privileged users.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.4 CONFIGURATION MANAGEMENT*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.4.1*** *Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.4 CONFIGURATION MANAGEMENT*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.4.2*** *Establish and enforce security configuration settings for information technology products employed in organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.4 CONFIGURATION MANAGEMENT*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.4.3*** *Track, review, approve/disapprove, and audit changes to organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.4 CONFIGURATION MANAGEMENT*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.4.4*** *Analyze the security impact of changes prior to implementation.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.4 CONFIGURATION MANAGEMENT*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.4.5*** *Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.4 CONFIGURATION MANAGEMENT*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.4.6*** *Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.4 CONFIGURATION MANAGEMENT*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.4.7*** *Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.4 CONFIGURATION MANAGEMENT*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.4.8*** *Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or denyall, permit-by-exception (whitelisting) policy to allow the execution of authorized software.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.4 CONFIGURATION MANAGEMENT*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.4.9*** *Control and monitor user-installed software.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.5 IDENTIFICATION AND AUTHENTICATION*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.5.1*** *Identify system users, processes acting on behalf of users, or devices.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.5 IDENTIFICATION AND AUTHENTICATION*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.5.2*** *Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.5 IDENTIFICATION AND AUTHENTICATION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.5.3*** *Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.5 IDENTIFICATION AND AUTHENTICATION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.5.4*** *Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.5 IDENTIFICATION AND AUTHENTICATION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.5.5*** *Prevent reuse of identifiers for a defined period.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.5 IDENTIFICATION AND AUTHENTICATION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.5.6*** *Disable identifiers after a defined period of inactivity.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.5 IDENTIFICATION AND AUTHENTICATION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.5.7*** *Enforce a minimum password complexity and change of characters when new passwords are created.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.5 IDENTIFICATION AND AUTHENTICATION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.5.8*** *Prohibit password reuse for a specified number of generations.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.5 IDENTIFICATION AND AUTHENTICATION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.5.9*** *Allow temporary password use for system logons with an immediate change to a permanent password.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.5 IDENTIFICATION AND AUTHENTICATION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.5.10*** *Store and transmit only cryptographically-protected passwords.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.5 IDENTIFICATION AND AUTHENTICATION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.5.11*** *Obscure feedback of authentication information.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.6 INCIDENT RESPONSE*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.6.1*** *Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.6 INCIDENT RESPONSE*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.6.2*** *Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.6 INCIDENT RESPONSE*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.6.3*** *Test the organizational incident response capability.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.7 MAINTENANCE*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.7.1*** *Perform maintenance on organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.7 MAINTENANCE*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.7.2*** *Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.7 MAINTENANCE*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.7.3*** *Ensure equipment removed for off-site maintenance is sanitized of any CUI.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.7 MAINTENANCE*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.7.4*** *Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.7 MAINTENANCE*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.7.5*** *Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.7 MAINTENANCE*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.7.6*** *Supervise the maintenance activities of maintenance personnel without required access authorization.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.8 MEDIA PROTECTION*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.8.1*** *Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.8 MEDIA PROTECTION*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.8.2*** *Limit access to CUI on system media to authorized users.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.8 MEDIA PROTECTION*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.8.3*** *Sanitize or destroy system media containing CUI before disposal or release for reuse.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.8 MEDIA PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.8.4*** *Mark media with necessary CUI markings and distribution limitations.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.8 MEDIA PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.8.5*** *Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.8 MEDIA PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.8.6*** *Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.8 MEDIA PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.8.7*** *Control the use of removable media on system components.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.8 MEDIA PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.8.8*** *Prohibit the use of portable storage devices when such devices have no identifiable owner.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.8 MEDIA PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.8.9*** *Protect the confidentiality of backup CUI at storage locations.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.9 PERSONNEL SECURITY*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.9.1*** *Screen individuals prior to authorizing access to organizational systems containing CUI.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.9 PERSONNEL SECURITY*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.9.2*** *Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.10 PHYSICAL PROTECTION*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.10.1*** *Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.10 PHYSICAL PROTECTION*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.10.2*** *Protect and monitor the physical facility and support infrastructure for organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.10 PHYSICAL PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.10.3*** *Escort visitors and monitor visitor activity.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.10 PHYSICAL PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.10.4*** *Maintain audit logs of physical access.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.10 PHYSICAL PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.10.5*** *Control and manage physical access devices.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.10 PHYSICAL PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.10.6*** *Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.11 RISK ASSESSMENT*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.11.1*** *Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.11 RISK ASSESSMENT*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.11.2*** *Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.11 RISK ASSESSMENT*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.11.3*** *Remediate vulnerabilities in accordance with assessments of risk.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.12 SECURITY ASSESSMENT*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.12.1*** *Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.12 SECURITY ASSESSMENT*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.12.2*** *Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.12 SECURITY ASSESSMENT*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.12.3*** *Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.12 SECURITY ASSESSMENT*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.12.4*** *Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.1*** *Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.2*** *Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.3*** *Separate user functionality from system management functionality.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.4*** *Prevent unauthorized and unintended information transfer via shared system resources.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.5*** *Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.6*** *Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.7*** *Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.8*** *Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.9*** *Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.10*** *Establish and manage cryptographic keys for cryptography employed in organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.11*** *Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.12*** *Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.13*** *Control and monitor the use of mobile code.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.14*** *Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.15*** *Protect the authenticity of communications sessions.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.13 SYSTEM AND COMMUNICATIONS PROTECTION*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.13.16*** *Protect the confidentiality of CUI at rest.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.14 SYSTEM AND INFORMATION INTEGRITY*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.14.1*** *Identify, report, and correct information and system flaws in a timely manner.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.14 SYSTEM AND INFORMATION INTEGRITY*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.14.2*** *Provide protection from malicious code at appropriate locations within organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.14 SYSTEM AND INFORMATION INTEGRITY*** |
| ***Basic Security Requirements*** |
| ***Security Control Requirement:***  ***3.14.3*** *Monitor system security alerts and advisories and take appropriate actions in response.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.14 SYSTEM AND INFORMATION INTEGRITY*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.14.4*** *Update malicious code protection mechanisms when new releases are available.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.14 SYSTEM AND INFORMATION INTEGRITY*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.14.5*** *Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.14 SYSTEM AND INFORMATION INTEGRITY*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.14.6*** *Monitor organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

|  |
| --- |
| ***3.14 SYSTEM AND INFORMATION INTEGRITY*** |
| ***Derived Security Requirements*** |
| ***Security Control Requirement:***  ***3.14.7*** *Identify unauthorized use of organizational systems.* |
| ***Security Control Implementation Details:***  [ ] Yes [ ] No [ ] Partially [ ] Does Not Apply [ ] Alternative Approach  **SECURITY PLAN AND PLAN OF ACTION QUESTIONS**  **How the Security Requirements are Implemented:**  <Answer accordingly.>  **How Any Unimplemented Security Requirements Will Be Met:**  <Answer accordingly.>  **How Any Planned Mitigations Will Be Implemented:**  <Answer accordingly.>  **How the Security Requirement is Partially Met:**  <Answer accordingly.>  **Why the Security Requirement Does Not Apply:**  <Answer accordingly.>  **The Alternative Approach that is Implemented:**  <Answer accordingly.> |

1. “Covered contractor information system” means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information. DFARS 252.204-7012(a). [↑](#footnote-ref-1)
2. “Covered defense information” means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is— (1)  Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract. DFARS 252.204-7012(a). [↑](#footnote-ref-2)
3. The latest version of NIST SP 800-171, called “Revision 1” is available at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf> [↑](#footnote-ref-3)