

UNCLASSIFIED

Body of Evidence for SystemName0

UNCLASSIFIED

Table of Contents

1. (U) System Information	1
2. (U) System Security Plan	2
3. (U) Security Assessment Report	6
4. (U) Risk Assessment Report	8
5. (U) Plan of Action and Milestones	10
6. (U) Authorization Decision Document	11

List of Tables

1. (U) External Security Services	3
2. (U) Security Control List	5
3. (U) Security Control Traceability List	7
4. (U) Test Results	7
5. (U) Threat Events	9

Chapter 1. (U) System Information

(U) System Name: SystemName0

(U) System Identifier: SystemIdentifier0

(U) System Version: SystemVersion0

(U) Organization Name: OrganizationName0

(U) Information Technology Type:

- Type of Service: ENCLAVE
- Is a Standalone System: True

(U) Security Categorization:

- **(U) Confidentiality:** MODERATE
- **(U) Integrity:** MODERATE
- **(U) Availability:** LOW

(U) System Short Name: SYSTEM

(U) National Security System: True

(U) Operational Environment: TEST

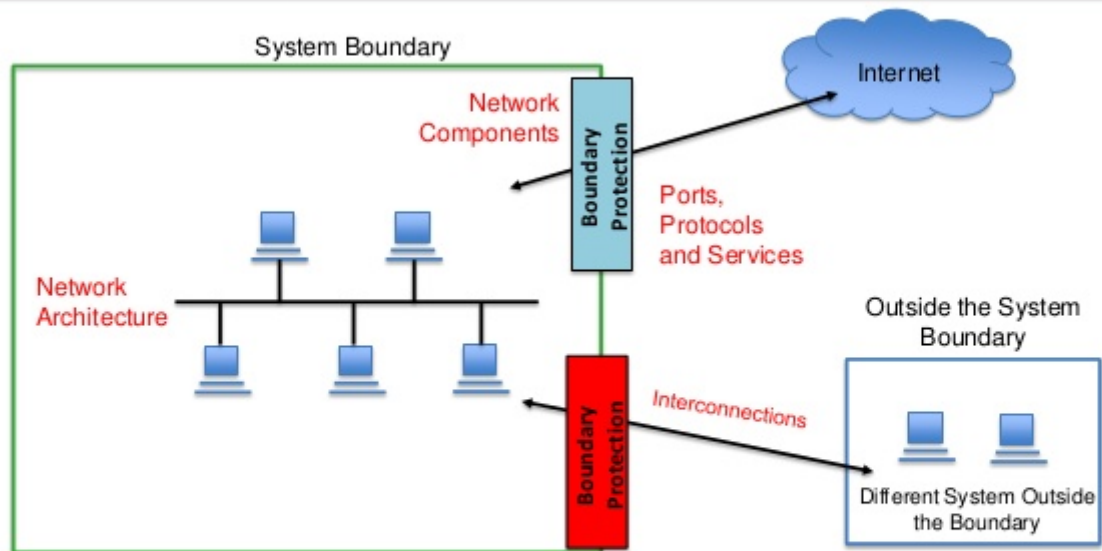
(U) Data Authorization Level:

- **Highest Classification Level:** UNCLASSIFIED
- **Authorized Handling Controls:** FOUO

Chapter 2. (U) System Security Plan

(U) Authorization Boundary Diagram: The following diagram is the Authorization Boundary Diagram and is UNCLASSIFIED.

Describing Boundaries in the System Security Plan (SSP)



- Understand which IT assets fit within the boundary.
- Interconnections - Indicate and label interconnections to other systems
- Indicate the hardware and software
- Make sure your diagrams are consistent with boundary descriptions

1111

(U) Image alt-text.

(U) Authorization Status: ATO

(U) Authorization Termination Date: 2020-05-04T18:13:51Z

(U) Cryptographic Key:

- **(U) FIPS Validated for Unclassified Information:** False -- This is a classified system, unclass validation not necessary.
- **(U) FIPS Validated for Compartmented Information:** True
- **(U) Uses NSA Approved Cryptography:** True

(U) E Authentication Assessment: False

(U) External Security Services: The following table is UNCLASSIFIED.

Table 1. (U) External Security Services

Service Name	Service Provider	Meets Organization Security Requirements?	Description
OAuth	Google	True	(U) blah blah blah

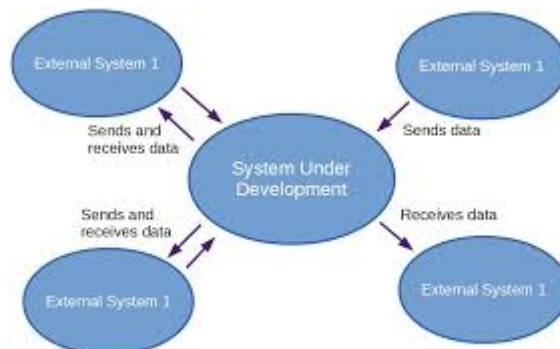
(U) Hardware Inventory:

- (U) Foo
 - **Manufacturer:** Bar
 - **Model Number:** 1G876

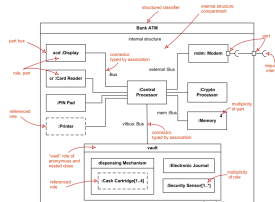
(U) Software Inventory:

- (U) Python
 - **Owner:** Python Software Foundation
 - **Version:** 3.1

(U) External System Interface Diagram: The following diagram is the External System Interface Diagram and is UNCLASSIFIED.

**(U) External Interface Diagram**

(U) Internal System Interface Diagram: The following diagram is the Internal System Interface Diagram and is UNCLASSIFIED.

**(U) Internal Interface Diagram**

(U) Network Connection Rules: NetworkConnectionRules0

(U) Information Type: Blah Blah Blah

(U) Information Flow Diagram: The following diagram is the Information Flow Diagram and is UNCLASSIFIED.



(U) Information Flow Diagram

(U) Mission Criticality: False

(U) System Ownership: GOVERNMENTOWNEDGOVERNMENTOPERATED

(U) Physical Environment: PhysicalEnvironmet0

(U) Key Roles:

- (U) Delegated Authorizing Official
 - **Name:** Gabriel Lorca
 - **Title:** Captain
 - **Organization:** Starfleet
 - **Phone:** 444-444-4444
- (U) Observer
 - **Name:** Michael Burnham
 - **Organization:** Starfleet
 - **Email:** michael.burnham@disco.sf.mil

(U) System Lifecycle Phase: 3-B-EMD

(U) System User Categories:

- (U) FEDERALSTATELOCAL:
 - (U) Access Description: General user access except for system administrators
 - User Constraints:
 - (U) User must have a TS clearance.
 - (U) User must be read into SI
 - (U) User must be read into TK
- (U) CONTRACTORS:
 - (U) Access Description: General user access except for system administrators
 - User Constraints:
 - (U) User must have a TS clearance.

- (U) User must be read into SI
- (U) User must be read into TK
- (U) **GENERALPUBLIC:**
 - (U) **Access Description:** No Access

(U) **Security Review Date:** 2017-12-07

(U) **System Function Description:** Blah blah blah

(U) **Security Control List:** The following table is UNCLASSIFIED.

Table 2. (U) Security Control List

Control Number	Control Name	Control Status	Implementation Description
AC-1	Access Control Policy and Procedures	IMPLEMENTED	(U) Access control policy and procedures are documented in lorem ipsum.
AC-2	Account Management	IMPLEMENTED	(U) Active Directory
AC-20	Use of External Information Systems	NOTAPPLICABLE	(U) Rationale: The system will be a standalone system and not be connected to external information systems.
AC-1	Audit and Accountability Policy and Procedures	PLANNED	(U) Current policy in draft, but expected to be signed before system enters production.

(U) **Applicable Overlays:**

- Intel

Chapter 3. (U) Security Assessment Report

(U) Assessment Date: 2017-10-26

(U) Sca Executive Summary: Executive summary from the detailed findings that are generated during a security control assessment. An executive summary provides an AO with an abbreviated version of the assessment report focusing on the highlights of the assessment, synopsis of key findings, and/or recommendations for addressing weaknesses and deficiencies in the security controls.

(U) Assessment Environment: Description of the environment where the most recent testing took place, including information on the site location and security system. Identify any supporting equipment (i.e. emulators, sniffers, analyzers, traffic generators, satellite simulators) that were used to support the assessment event, and list any external interfaces active during the test even. Explain any constraints imposed by the environment on the assessment event which impacted on the quality or quantity of testing able to be performed. Identify all personnel present for the assessment, their organizations, and their role in the assessment event. Resource: test results report.

(U) Assessment Methodology: Identifies methodology and procedures used to assess controls (e.g, NIST SP 800-53A, DoD Joint Security Implementation Guide). If other methodology or procedures were used, provide rationale for deviation from standards assessment resources.

(U) Assessment Objective Type: Independent verification and validation.

(U) Security Assessor:

- **Name:** Ash Tyler
- **Title:** Lieutenant

(U) Constraints And Issues:

- **(U) Assumption List:**
 - **Assumption:** Assumption1
 - **Assumption:** Assumption2
- **(U) (U) Constraint List:**
 - **(U) Constraint:** Constraint1
 - **(U) Constraint:** Constraint2
- **(U) Issue List:**
 - **Issue:** Issue1
 - **Issue:** Issue2

(U) (U) Components Assessed:

- **(U) Component Identifier:** Comp1
- **(U) Component Identifier:** Comp2

(U) Security Control Traceability List: The following table is UNCLASSIFIED.

Table 3. (U) Security Control Traceability List

Control Number	Requirement ID
AC-1	1.2.3.4
AC-2	1.2.3.5

(U) Test Results: The following table is UNCLASSIFIED.

Table 4. (U) Test Results

Test ID	Test Date	Resource Tested	Control Number Tested	Test Result
1A	2017-10-20	system0	AC-1	Passed
1B	2017-10-20	system0	AC-2	Failed

Chapter 4. (U) Risk Assessment Report

(U) Assessment Date: 2017-10-26

(U) Risk Assessment POC:

- **Name:** Saru
- **Email:** saru2@disco.sf.mil

(U) Purpose For Risk Assessment: Describe the purpose of the risk assessment. The purpose may be to determine risk at various system life cycle phases, to include the security categorization, to tailor security controls, to assess the risk of non-compliant security controls, to assess the impact of actual or proposed changes to the system in operations, etc.

(U) Risk Assessment Scope: The scope of the risk assessment can be at any of the three tiers in the risk management hierarchy (i.e., organization, mission/business process, or system), or the scope can be limited to certain portions of the system. Identify scope of assessment including boundaries and intended mission(s) the system is designed to support

(U) Risk Assessment Summary: Executive summary from the detailed findings generated during risk assessment. An executive summary provides an AO with an abbreviated version of the risk assessment report focusing on the highlights of the assessment, purpose, synopsis of key findings, and/or recommendations for addressing risk.

(U) Organizational Risk Tolerance: Risk Tolerance (including a list of the range of consequences to be considered) –The level of risk an entity is willing to assume in order to achieve a potential desired result; Identify any organization risk tolerance levels set at Tier 1, Tier 2, and Tier 3

(U) Overall Risk Posture: MODERATE

(U) Overall Risk Ratings:

- **Very Low:** 15
- **Low:** 5
- **Moderate:** 3
- **High:** 1
- **Very High:** 2

(U) Risk Analysis Approach: THREAT

(U) Risk Assessment Approach: SEMI-QUALITATIVE

(U) Threat Events: The following table is UNCLASSIFIED.

Table 5. (U) Threat Events

Event	Vulnerabilities	Sources	Likelihood of Occurrence	Likelihood of Success	Overall Likelihood	Residual Risk Level
The threat event by name.	Vulnerability1 Vulnerability2	Source1	LOW	VERY_LOW	LOW	LOW
The threat event by description.	Vulnerability3	Source2	LOW	VERY_LOW	LOW	VERY_LOW
The threat event by reference.	Vulnerability4	Source1	HIGH	VERY_HIGH	MODE RATE	LOW

Chapter 5. (U) Plan of Action and Milestones

(U) Assessment Date: 2017-09-26

(U) Deficiency:

- **(U) Name:** My Deficiency
- **(U) Description:** Bad things.

(U) Completion Status: ONGOING

(U) Scheduled Completion Date: 2017-10-25

(U) Completion Date: 2017-10-27

(U) Point Of Contact:

- **Name:** Paul Stamets
- **Email:** paul.stamets@disco.sf.mil

(U) Applicable Security Control: AC-1

(U) Identifying Event:

- **(U) Event:** Power outage
- **(U) Reviewing Organization:** MIA/IAD

(U) Comments: Additional detail, clarifications, or other commentary.

Chapter 6. (U) Authorization Decision Document

(U) Authorization Decision: ATO

(U) Authorizing Official:

- **Name:** Gabriel Lorca
- **Title:** Captain

(U) Authorization Decision Date: 2017-10-31

(U) Authorization Decision Termination Date: 2020-10-31

(U) Authorization Terms And Conditions: Provides a description of any specific limitations or restrictions placed on the operation of the system.

(U) Risk Executive Input: The security related-considerations from the Risk Executive which the AO deems relevant and affects the final authorization decision. These considerations are viewed from organization-wide perspective with regard to the overall strategic goals and objectives in carrying out the mission and business functions. (e.g., organizational risk tolerance, organization's overall risk mitigation strategy, core mission and business requirements, dependencies among systems, ongoing risk monitoring requirements, and other types of risks not directly associated with the system or its environment of operation).

(U) Overall Risk Ratings:

- **Very Low:** 15
- **Low:** 5
- **Moderate:** 3
- **High:** 1
- **Very High:** 2