PROGRAM NAME

SCIENCE AND TECHNOLOGY (S&T) PROTECTION PLAN

VERSION

DATE

****

Introduction (Instructional; Not for Inclusion in S&T Protection Plan)

This sample S&T Protection Plan Template is intended to inform S&T Managers regarding example best practices that may be adapted to meet unique organizational needs and program requirements. The following questions and tables have been provided to suggest a tailorable series of topics that may be covered throughout the S&T protection process. Program-specific requirements will dictate which topics and questions are applicable and potentially introduce new ones. Therefore, S&T Managers are free to edit or tailor portions of this template as needed to suit agency requirements or the purposes of individual projects. This document is not a checklist, but rather is intended to facilitate discussions between S&T Managers, Technology SMEs, Security Staffs, Counterintelligence Representatives, and Intelligence Analysts that account for a wide range of threat scenarios while formulating appropriate countermeasures.

As identified in Department of Defense (DoDI) 5000.83, the S&T Protection Plan must document, at a minimum, (1) critical technology elements and enabling technologies, (2) threats to, and vulnerabilities, of these items, and (3) selected countermeasures to mitigate associated risks. This template recommends the following five sections intended to address these requirements and provide an iterative record of risk management over the program's lifecycle:

1. *Introduction, Updates, and Responsible Points of Contact (POCs)*
2. *Technology Element Identification and Risk Assessment*
3. *Identified Threats and Vulnerabilities*
4. *Countermeasures and Risk Mitigation Plan*
5. *Response, Recovery, and Support*

S&T Protection Plan Update Record

Guidance: Update the following table listing S&T Protection Plan updates, as necessary.

S&T Protection Plan Update Record

Revision Number	Date	Changes	Approved By

Contents

1. Introduction, Updates, and Responsible POCs

1.0.1 Program Purpose and Description

Enter Text Here

Guidance: Provide a description and describe the purpose of the program that will be addressed by this Protection Plan.

1.0.2 Timing and Approval Authorities for S&T Protection Plan updates

Enter Text Here

Guidance: Describe the timing of S&T Protection Plan updates (e.g., prior to milestone, prior to export decision, following Systems Engineering Technical Review) and applicable approval authorities.

Table 1.0.2-1 Timing and Approval Authorities (sample)

Action	Milestone	Approval Authority
Initial Draft	Program approval	
Final Version	Broad Agency Announcement (BAA) release	
Update	Source selection	
Update	60 days after program kick-off	
Update	Annual Review	
Update	Technology Transition Agreement drafted	

1.1.0 Responsible POCs for the Program

Enter Text Here

Guidance: Identify the lead personnel who will be responsible for implementing countermeasures.

Table 1.1-1 S&T Protection Plan Government POCs (sample)

Title/Role	Name	Contact Info	Organization
S&T Manager			
Lead Systems Engineer			
S&T Protection Lead			
Physical Security Manager			

IT Security Manager			
Transition Partner			
Contracting Officer			

Table 1.1-2 S&T Protection Plan Performer POCs (sample)

Title/Role	Name	Citizenship	Contact Info
Research Participant			
IT Security Manager			

2. Technology Element Identification and Risk Assessment

Guidance: List the technology elements contained in the program (Open, CUI, Export Controlled, etc.) as identified during the completion of the Fundamental Research Review and Technology Element Identification Questions. For each element, describe the impact of the loss, theft, or compromise of related information on the program as well as related programs. S&T Managers should coordinate with security staffs and CI and intelligence personnel while utilizing resources such as the Office of the Secretary of Defense for Research and Engineering (OUSD(R&E)) Technology Area Protection Plans (TAPPs), List of Critical Programs and Technologies for Prioritized Protection, Horizontal Protection Guides (HPGs) (e.g., Low Observable/Counter Low Observable (LO/CLO) Security Classification Guide (SCG), DoD Critical Program Information (CPI) HPG, Hypersonics for Military Systems and Applications SCG, etc.), and organizational SCGs to complete the impact assessment.

Table 2.0-1 Technology Element Identification and Risk Assessment (sample)

Research Element	**Control Description** (Open, CUI, Export Controlled, etc.)	**Classification** (C, S, TS)	**Impact to Warfighter**
Element 1	**Open**		
Enabling technology 1.1	Open		
Enabling technology 1.2	Open		

Enabling technology 1.3	Open		
Element 2	**CUI, Export Controlled**		(**CRITICALITY DEFINITION**). Short description of impact on program and related programs.
Enabling technology 2.1	CUI, Export Controlled		
Enabling technology 2.2	Open		
Enabling technology 2.3	CUI, CTI		
Element 3	**Export Controlled**	**S**	
Enabling technology 3.1	CUI		
Enabling technology 3.2	CUI		
Enabling technology 3.3	CUI, Export Controlled		

3. Identified Threats and Vulnerabilities

Guidance: S&T Managers should coordinate with security staffs and CI and intelligence personnel while utilizing resources such as the OUSD(R&E) Technology Area Protection Plans (TAPPs), List of Critical Programs and Technologies for Prioritized Protection, Horizontal Protection Guides (e.g., LO/CLO SCG, DoD CPI HPG, Hypersonics for Military Systems and Applications SCG, etc.), and organizational Security Classification Guides to determine applicable threats and vulnerabilities.

3.1.0 Program-Specific Threats and Vulnerabilities

Enter Text Here

Guidance: Describe any threats (e.g., adversary collection methods) specific to or assessed as more likely given the program's content or intent.

3.2.0 Threats Specific to State Actors

Enter Text Here

Guidance: List any technology elements or areas contained in the program that may be tied to the interests of a specific state actor.

3.2.1 Threats Specific to State Actors – Technology Elements & Enabling Technologies

Enter Text Here

Guidance: Assess the likelihood that the loss, theft, or compromise of information related to critical technology elements or enabling technologies would likely result in foreign adversaries filling critical technology gaps.

3.2.2 Threats Specific to State Actors – Controlled Unclassified Information

Enter Text Here

Guidance: Assess the likelihood that the unauthorized disclosure of CUI elements would likely result in foreign adversaries filling critical technology gaps.

3.2.3 Threats Specific to State Actors – Classified Information

Enter Text Here

Guidance: Assess the likelihood that the loss, theft, or compromise of classified information elements would likely result in foreign adversaries filling critical technology gaps.

4. Countermeasures and Risk Mitigation Plan

4.1.0 Personnel

4.1.1 Personnel - Access

Enter Text Here

Guidance: Describe the process that will be utilized to grant and document access for personnel who will actively work on the program.

4.1.2 Conflicts of Interest (CoI) and Commitment (CoC)

Enter Text Here

Guidance: Describe the methods that will be utilized to identify and resolve reported or discovered conflicts of interest and/or commitment.

4.1.3 Foreign Visits Accountability Plan

Enter Text Here

Guidance: Describe the process that is being utilized to track and maintain accountability for foreign visits.

4.1.4 Foreign Travel Accountability Plan

Enter Text Here

Guidance: Describe the process that is being utilized to track and maintain accountability for foreign travel.

4.2.0 Foreign Involvement

4.2.1 International Cooperative Development Activities

Enter Text Here

Guidance: Describe any planned, existing, or anticipated international cooperative development activities related to the program.

4.2.2 Foreign Vendor Engagements and Procurements

Enter Text Here

Guidance: Describe how planned, existing, and anticipated foreign vendor engagements and procurements of critical products and services are reviewed for risk (e.g. malicious software, hardware, deemed exports, unauthorized disclosure, etc.)? How are such engagements documented?

4.3.0 Training

4.3.1 Critical Technology Elements

Enter Text Here

Guidance: Describe the training conducted to inform personnel about safeguarding critical technology elements. Additionally, identify the resources utilized to develop the training.

4.3.2 Controlled Unclassified Information (CUI)

Enter Text Here

Guidance: Describe the training conducted to inform personnel about safeguarding CUI. Additionally, identify the resources utilized to develop the training.

4.3.3 Insider Threat

Enter Text Here

Guidance: Describe the training conducted to inform personnel regarding insider threats as they relate to the program. Additionally, identify the resources utilized to develop the training.

4.3.4 Export Control

Enter Text Here

Guidance: Describe the training conducted to inform personnel regarding export control policies, if applicable. Additionally, identify the resources utilized to develop the training.

4.3.5 Training - Resources

Enter Text Here

Guidance: Identify the resources utilized to develop each training program.

4.3.6 Training - Schedule

Enter Text Here

Guidance: Identify how often each required training is conducted.

4.3.7 Training - Documentation

Enter Text Here

Guidance: Describe the process that is in place for tracking the completion of training.

4.4.0 Information Technology

4.4.1 NIST SP 800-171 Compliance

Enter Text Here

Guidance: Identify whether systems that will be utilized over the course of the program are compliant with NIST SP 800-171 requirements.

4.4.2 NIST SP 800-171 Non-Compliance – Risk Mitigation Plan

Enter Text Here

Guidance: Identify non-compliant systems, actions taken to mitigate risk and seek compliance, and timelines for compliance.

4.4.3 IT Systems - Transportation

Enter Text Here

Guidance: Describe the policy that will be utilized regarding the transport of IT systems away from the work site, to include possible restrictions.

4.4.4 Personal Electronic Device Policy

Enter Text Here

Guidance: Describe what policies are in place regarding the use of personal electronic devices in the vicinity of work sites, if any.

4.4.5 Attribution Methods

Enter Text Here

Guidance: Describe what attribution methods will be utilized to ensure the accountability and integrity of research data and CUI (e.g., digital identifiers).

4.5.0 Physical Security

4.5.1 Physical Access to Systems and Information

Enter Text Here

Guidance: Describe the measures that are in place to prevent physical access to information and systems by unauthorized personnel.

4.5.2 Document and Media Storage

Enter Text Here

Guidance: Describe the measures that will be implemented regarding physical document and electronic media storage, container type, and access controls.

4.5.3 Transport and Shipment

Enter Text Here

Guidance: Describe the measures that will be implemented regarding the physical transportation and shipment of documents, materials, technology, systems, etc.

4.5.4 Document Destruction

Enter Text Here

Guidance: Describe the measures that will be implemented regarding physical document destruction.

4.6.0 Program-Specific Countermeasures

4.6.1 Unique Protections

Enter Text Here

Guidance: Describe whether specific technology elements require unique protections not applicable to the program as a whole.

4.6.2 International Traffic in Arms Regulations (ITAR) & Export Administration Regulations (EAR)

Enter Text Here

Guidance: Describe how ITAR and EAR procedures will be documented and applied to the program, if required.

4.7.0 Horizontal Protection

4.7.1 Horizontal Protection Plan

Enter Text Here

Guidance: Describe the process that is in place for protecting critical technology elements or enabling technologies that have applications across multiple domains or priorities.

4.7.2 Horizontal Protection – External POCs

Enter Text Here

Guidance: List points of contact that have been identified for protection coordination.

4.8.0 Emerging Threats and Vulnerabilities

4.8.1 Emerging Threats and Vulnerabilities Plan

Enter Text Here

Guidance: Describe the plan that will be utilized to maintain awareness of emerging threats and vulnerabilities as they relate to the program.

4.8.2 Emerging Threats and Vulnerabilities Plan - Integration

Enter Text Here

Guidance: Describe the process that will be utilized to integrate knowledge of emerging threats and vulnerabilities into the existing S&T Protection Plan.

4.9.0 Test Planning, Experimentation, and Evaluation Outside of Protected Environments

4.9.1 Exceptions

Enter Text Here

Guidance: Identify any portion of the program that involves elements of testing or evaluation that require an exception to outlined protection requirements.

4.9.2 Exceptions – Risk Mitigation

Enter Text Here

Guidance: Describe the process that will be utilized to mitigate previously identified threats or vulnerabilities under these conditions.

4.10.0 Technology Transition Plan

4.10.1 Method of Transition

Enter Text Here

Guidance: Describe whether it is anticipated that technology elements will be transitioned as component technologies, sub-component technologies, or a complete system.

4.10.2 Transition Partners

Enter Text Here

Guidance: List any transition partners that have been identified for this program (Program Executive Offices (PEOs), Combat Capability Development Centers (CCDCs), Industry partners, etc.).

4.10.3 Security Requirements

Enter Text Here

Guidance: Describe any security-relevant transition/mission partner requirements that the program needs to incorporate into a technology transition plan (security classification changes, anti-tamper requirements, OPSEC considerations or association concerns, etc.)

4.10.4 Signed Agreements and Risks

Enter Text Here

Guidance: Is there a signed Transition Agreement (TA), Technology Transfer Agreement (TTA), Memorandum of Agreement (MOA), or Memorandum of Understanding (MOU) governing the transition agreement between the S&T organization and the transition/mission partner? If so, are critical risks and security-relevant requirements specified in said agreement?

4.10.5 Intellectual Property

Enter Text Here

Guidance: Describe any intellectual property (e.g., technical data and computer software deliverables, patented technologies and associated license rights, etc.) that is required to support acquisition and sustain the product lifecycle for the recipient. If applicable, identify where intellectual property elements will be located and the entities responsible for those elements.

4.10.6 Intellectual Property (Government)

Enter Text Here

Guidance: Describe any intellectual property rights pertaining to the government. If applicable, identify where intellectual property elements will be located and the entities responsible for those elements.

4.10.7 Data Rights

Enter Text Here

Guidance: Describe any data rights that are required (unlimited, government purpose, restricted, or limited). If applicable, identify the entities that will maintain these data rights.

4.11.0 Published Work and Public Communications Plan

4.11.1 Disclosure Mitigation

Enter Text Here

Guidance: Identify any guidelines in place to protect critical technology elements from disclosure through publishing or communications with the public.

4.11.2 Public Affairs Plan

Enter Text Here

Guidance: Describe the public affairs plan in place to communicate program details while limiting unauthorized disclosure.

4.11.3 Pre-Publication Review

Enter Text Here

Guidance: Describe the process that will be utilized for pre-publication review.

5. Response, Recovery, and Support

5.1.0 Reporting Requirements

5.1.1 Response Coordination

Enter Text Here

Guidance: List the Personnel Security (PERSEC) Managers, Information Security (INFOSEC) Managers, Foreign Disclosure Representatives, and Export Control Representatives who have been identified as POCs for response coordination.

5.1.2 Reporting

Enter Text Here

Guidance: Describe the reporting instructions that will be utilized to coordinate with counterintelligence, security, and law enforcement POCs regarding breaches of protection policies.

5.2.0 Remediation

5.2.1 Unauthorized Disclosure

Enter Text Here

Guidance: Describe the policies that are in place to ensure appropriate action is taken for violation of disclosure requirements.

5.2.2 Security Systems

Enter Text Here

Guidance: Describe the policies that are in place to respond to intentional penetrations of cyber and physical security systems.