BY ORDER OF THE COMMANDER
AIR FORCE RESEARCH LABORATORY
(AFRL)

AIR FORCE RESEARCH LABORATORY
INSTRUCTION 61-113

3 JUNE 2022

Scientific/Research and Development

SCIENCE AND TECHNOLOGY PROTECTION FOR THE AIR FORCE RESEARCH LABORATORY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AFRL/EN & AFRL/DSI

Certified by: AFRL/CA
(Mark A. Dipadua)

Supersedes: AFRLI63-113, 1 May 2018

Pages: 41

This instruction implements DoDI 5000.83, *Technology and Program Protection to Maintain Technological Advantage'* DAFPD61-1, *Management of The Science and Technology Enterprise, and* AFI61-101, *Management of Science and Technology*. This instruction applies to all classified and unclassified DoD-funded research and development (R&D) that is conducted by AFRL, henceforth referred to as "S&T efforts". Special Access Programs (SAP), Sensitive Compartmented Information (SCI) programs, and non-collateral programs, as well as collateral portions of these programs shall comply with this instruction. Nothing in this issuance alters or supersedes the existing authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartment information, as directed by Executive Order 12333 and other laws and regulations. This publication may be supplemented at any level, but all supplements must be routed to the office of primary responsibility (OPR) of this publication for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication; route AF Forms 847 through appropriate chain of command. References to the authority to waive requirements in this publication resides with the AFRL Vice Commander (CV). Submit requests for waivers through the chain of command to the Publication OPR for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

SUMMARY OF CHANGES

The change of publication series from AFRLI63-113 to AFRLI61-113 was accomplished to properly align with the current Air Force (parent) publications and to ensure the publication is attuned with the correct subject matter series.

1. Overview/Purpose.

1.1. This instruction implements DoDI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*. This instruction provides AFRL Science and Technology (S&T) Managers, S&T Protection Leads, and supporting technical personnel with required planning activities and procedures for protecting AFRL S&T. This instruction implements DoDI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*. This document incorporates recent OSD guidance (DoDI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*) which directs increased protection for all DoD-sponsored research and technology that is in the interest of national security. Among other provisions, DoDI 5000.83 directs DoD personnel to conduct initial and annual reviews of all S&T activities to assess the risk of adversarial exploitation of S&T efforts. Further, this guidance directs all organizations to take necessary actions to incorporate risk assessments as a standard part of the S&T acquisition and assistance processes.

1.2. Previous AFRL protection policy (AFRLI 63-113, *Program Protection Planning for the Air Force Research Laboratory*) directed protection of Controlled Unclassified Information (CUI) through establishment of Program Protection Plans (PPP). While this approach provided ample protections for data identified as CUI, DoDI 5000.83 has directed the extension of protections "beginning with early S&T investment and continuing throughout the entire Defense Acquisition Lifecycle." In accordance with (IAW) this provision, this instruction rescinds the requirement for PPPs and directs the establishment of S&T Protection Plans. S&T Protection Plans differ from PPPs in that they (a) annually identify all Critical Technology Elements (CTE) and (b) establish a set of S&T tailored protection measures to ensure a comprehensive approach across all S&T efforts.

1.3. This instruction has several objectives. First, it provides guidance for how S&T Managers, S&T Protection Leads, and supporting personnel implement S&T protection as part of the S&T acquisition or assistance process. Second, it includes guidance for identification and categorization of AFRL CTEs as part of the annual S&T protection process. Finally, this instruction outlines essential content of the S&T Protection Plan and directs utilization of AFRL Core Technical Competencies (CTC) or other HQ AFRL-approved structures as the organizational framework for these plans. Tools, templates, and checklists are provided to assist the S&T protection teams in execution of these measures. Digital versions of these are located on the AFRL/DSI SharePoint site (**https://usaf.dps.mil/teams/10722/InfoPro/SitePages/Science%20and%20Technology.aspx**).

2. Roles and Responsibilities.

2.1. **AFRL Commander (AFRL/CC).**

2.1.1. Will provide policy and guidance for the implementation and application of S&T Protection.

2.1.2. Will serve as principal responsible authority for implementation and review of all S&T protection measures across the AFRL Enterprise. This responsibility may be delegated as appropriate to meet the objectives of this instruction.

2.2. **AFRL Engineering and Technical Management Directorate (AFRL/EN) and AFRL Information Protection (AFRL/DSI).**

2.2.1. Will host a recurring AFRL S&T Protection Working Group to exchange S&T Protection strategies and best practices across the AFRL enterprise.

2.2.2. Will maintain and protect a repository for AFRL CTEs.

2.2.3. Will report CTE and other protection information to OUSD and other Services as required to facilitate horizontal protection of technologies.

2.2.4. Will host crosstalk discussions with AFRL leadership to resolve horizontal protection discrepancies.

2.3. **Mission Organization (Msn Org) Director.**

2.3.1. Will appoint either the Chief Engineer or Chief Scientist as the Msn Org's S&T Protection Working Group Chair.

2.3.2. Will appoint an engineering/technical S&T Protection Lead and a security S&T Protection Lead.

2.4. **S&T Protection Working Group Chair.**

2.4.1. Will maintain a listing of the Msn Org's current S&T Protection Plans, S&T Protection Plan Annexes, and their S&T Managers/Owners.

2.4.2. Will review all directorate S&T Protection Plans to ensure content is accurate and complete.

2.4.3. Will serve as the approval authority for S&T Protection Plans.

2.4.4. Will be the final decision authority for identification and protection of all CTE.

2.4.5. Will maintain the Msn Org's current CTE list and submit to HQ AFRL annually.

2.4.6. Will designate all members of the S&T Protection Working Group as either required or optional.

2.5. **S&T Protection Working Group.**

2.5.1. Will be composed of functional and technical experts who review the Msn Org's S&T portfolio to validate candidate CTE. S&T Protection Working Group members, and their designees, should be seasoned professionals with S&T and/or S&T protection experience. The S&T Protection Working Group will consist of required and optional members. At a minimum, S&T Protection Plan owners, engineering and security S&T Protection Leads, and the S&T Protection Working Group Chair are among the required members. Information System Security Managers or Officers (ISSM or ISSO), Foreign Disclosure Officers (FDO), and Contracting Professionals are examples of optional members.

2.5.2. Will review the results from the CTE Identification Worksheet for all programs identified as containing candidate CTE. The S&T Protection Working Group, with the S&T Protection Working Group Chair's approval, will validate the candidate CTEs to be included in the Msn Org's CTE list and in a CTC-level S&T Protection Plan.

2.5.3. Will convene, at a minimum, semi-annually. All required members of the S&T Protection Working Group or their designees must participate in order to convene a meeting. Optional members might only participate in a consultant capacity. The S&T Protection Working Group must maintain minutes and action items for the meetings.

2.6. **Core Technical Competency (CTC)-level S&T Protection Plan Owners.**

2.6.1. Will develop an overarching S&T Protection Plan for their CTC, sub-CTC, or other HQ AFRL-approved structure which, per DoDI 5000.83, includes CTE and enabling technologies. Also required are threats to and vulnerabilities of these items, and selected countermeasures to mitigate associated risks.

2.6.2. Will coordinate with S&T Managers who conduct efforts within their CTC to identify all candidate CTE to be presented to the S&T Protection Working Group.

2.6.3. Will ensure that CTE is adequately decomposed to provide protection at the lowest level required.

2.6.4. Will review their S&T Protection Plan annually and update as required to ensure proper protection of AFRL CTE and enabling technologies.

2.6.5. Will assist S&T Managers in creation of annexes, as required.

2.7. **S&T Manager (This role can be filled by R&D Program Managers, Program Officers, Project Leads, Engineers, or others that manage science and/or technology projects.**)

2.7.1. Will conduct, in coordination with S&T Protection Lead, an initial and annual risk assessment of their effort using the procedures outlined in Section 3.4 of this document.

2.7.2. Will use information from initial and annual risk assessments to make risk-informed decisions about the future of their effort.

2.7.3. Will annually review, in coordination with S&T Protection Lead, all relevant protection plans, including, but not limited to, AFRL S&T Protection Plans, AFRL or Customer PPPs, OUSD Technology Area Protection Plans (TAPP), and OUSD Critical Programs and Technologies (CP&T) list.

2.7.4. Will develop, in coordination with S&T Protection Lead and CTC-level S&T Protection Plan owner, an S&T Protection Plan Annex and/or standalone S&T Protection Plan if additional protection is required.

2.7.5. Will clearly communicate CTE and protection measures to customers, stakeholders, and collaborators, with proper distribution statements/classification and/or permission.

2.7.6. Will ensure that any collaborative materials that are marked Distribution A are cleared by Public Affairs prior to dissemination.

2.7.7. Will ensure, in coordination with contracting/agreements/grants officer, that solicitations (e.g., RFPs, BAAs) include requirements to deliver a Standard Form 424 (SF 424), *Research and Related Senior/Key Person Profile (Expanded) Form*, or equivalent form and Security Program Questionnaire with each proposal.

2.7.8. Will ensure, in coordination with contracting/agreements/grants officer, that solicitations (RFPs, BAA, etc.) include evaluation criteria for S&T protection, including evaluation of personnel conflicts of interest (CoI) and conflicts of commitment (CoC).

2.7.9. Will ensure, in coordination with contracting/agreements/grants officer, all AFRL research efforts (contracts, grants, agreements, OTs, etc.) include requirements to deliver an up-to-date SF 424, *Research and Related Senior/Key Person Profile (Expanded) Form,* annually or when personnel changes occur.

2.7.10. Will review initial/annual SF 424, *Research and Related Senior/Key Person Profile (Expanded) Form,* in coordination with contracting/agreements/grants officer to identify risks or CoI/CoC. Any concerns will be directed to S&T Protection Lead.

2.7.11. Will ensure, in coordination with contracting/agreements/grants officer, the S&T Protection Plan is included with all contracts, agreements, and grants involving CTE or enabling technologies.

2.7.12. Will provide updates to CTC-level S&T Protection Plan when new CTE or new threats are identified.

2.7.13. Will inform all government and non-government team members of protection of CTE within 30 calendar days following identification of new CTE, upon arrival of new personnel, and annually thereafter, with proper distribution statements/classification and/or permission.

2.7.14. Will ensure incidents of loss, compromise, or theft of identified CTE are immediately reported to the S&T Protection Lead within 72 hours.

2.8. **S&T Protection Leads.**

2.8.1. Will coordinate closely with S&T Managers to determine all S&T protection requirements.

2.8.2. Will lead the development of all S&T Protection Plans. Will provide S&T Managers and S&T Protection Plan owners with appropriate guidance, templates, and outlines to assist in the development of S&T Protection Plans.

2.8.3. Will determine, in coordination with the S&T Manager and S&T Protection Plan owner, the need for an annex or standalone S&T Protection Plan when existing S&T Protection Plans are not sufficient to cover an effort's protection needs.

2.8.4. Will review and provide feedback on research performers listed in initial and annual SF 424, *Research and Related Senior/Key Person Profile (Expanded) Form,* as requested by the S&T Manager. In case of unresolved concerns, S&T Protection Leads will contact AFRL S&T Protection Functionals. Additional reviews can be conducted by the AFRL Foreign Influence Risk Management and Advisement Team.

2.8.5. Will ensure that S&T Managers have access to templates, checklists, tools, etc. to make risk-based decisions about the future of their efforts.

2.8.6. Will maintain all Msn Org S&T protection documentation in a central location, to include documentation (decisions, minutes, action items, etc.) of S&T Protection Working Group meetings and a repository of completed CTE Identification Worksheets.

2.8.7. Will assemble all applicable CTE Assessments for the S&T Protection Working Group meetings and document the minutes and decisions.

2.8.8. Will be the Msn Org focal point for all inspections involving S&T Protection. The S&T Protection Leads must have the basic ability to converse technical aspects of S&T Protection and explain the process and how it fits into the overall technical mission.

2.8.9. Will coordinate with the contracting community and S&T Managers (when applicable) to ensure contracts and solicitations are written to address all S&T protection requirements.

2.8.10. **Engineering S&T Protection Lead**

2.8.10.1. Will oversee identification of CTE and ensure that CTE is properly decomposed to prevent both over- and under- protection.

2.8.11. **Security S&T Protection Lead**

2.8.11.1. Will assist with coordinating support of AFOSI and Intelligence agencies, facilitating accomplishment of threat assessment requests.

2.8.11.2. Will assist the CTC leads and S&T Managers with the review of the Integrated Threat Assessment (ITA) and generation of threat sections for S&T Protection Plans.

2.8.11.3. Will assist the S&T Manager with training requirements from S&T Protection Plans when necessary.

2.8.11.4. Will ensure that Department of Defense Form 254 (DD 254), *Contract Security Classification Specification*, is used for classified efforts with appropriate security guidance in order to communicate S&T Protection Plan requirements to contractors. Center industrial security will facilitate standard verbiage and requirements across AFRL.

2.8.11.5. Will oversee OPSEC procedures within their assigned portfolio, to ensure appropriate OPSEC requirements are followed.

2.9. **AFRL Foreign Influence Risk Management and Advisement Team.**

2.9.1. Will assist in conducting security deep dives that are above and beyond the capacities of Msn Org Security/Technical S&T Protection Leads.

2.10. **Information System Security Manager (ISSM) or Information System Security Officer (ISSO).**

2.10.1. Will assist S&T Managers in determining the appropriate and required countermeasures to protect CTE residing on information systems.

2.10.2. Will ensure these countermeasures are clearly identified/documented in the Risk Management Framework (RMF) Assessment and Authorization (A&A) package and referenced in the S&T Protection Plan.

2.10.3. Will ensure any system processing, storing, or transmitting government information, to include CTE, will undergo RMF A&A activities based on the Confidentiality, Integrity, and Availability impact values of the system.

2.10.4. Will ensure these systems comply with RMF A&A Continuous Monitoring and/or Change Management.

2.11. **Contracting/Agreements/Grants Officers and/or Buyers.**

2.11.1. Will include protection language in all solicitations, including requests for an initial SF 424, *Research and Related Senior/Key Person Profile (Expanded) Form*, and Security Program Questionnaire as part of the proposal package and evaluation criteria for S&T protection.

2.11.2. Will review SF 424, *Research and Related Senior/Key Person Profile (Expanded) Form*, in coordination with the S&T Manager to identify and mitigate/correct S&T protection risks or CoIs/CoCs before award.

2.11.3. Will coordinate with S&T Managers and S&T Protection Leads to identify appropriate S&T protection language for each effort (e.g., deliverables, requirements for adherence to S&T Protection Plans, training, CDRLs, DD Form 254, AFRL Form 191).

2.12. **AFRL Senior Intelligence Officers (SIO).**

2.12.1. Will provide support to the S&T Manager in assessing threats within regulatory limitations, to include Intelligence Oversight.

2.12.2. Will ensure intelligence products are generated and provided to the S&T Manager as appropriate for the situation.

3. Procedure.

3.1. S&T Protection is an annual review process for identifying CTE and risks to AFRL S&T; and selecting cost-effective mitigation strategies to ensure protection throughout the technology lifecycle. The S&T protection team includes experts from various functional disciplines including S&T Managers, S&T Protection Leads, intelligence, counterintelligence, and contracting. The process provides a comprehensive approach to assess and balance risks from available threat data and partner review. These risks shall include, but may not be limited to, inadvertent, negligent, or intentional compromise and/or loss of S&T information. Risk identification, assessment, and established countermeasures are documented in S&T Protection Plans to ensure all AFRL personnel and AFRL partners understand, implement, and communicate protection measures for AFRL efforts. The initial and annual process overview is shown in Figures **1 and 2**.

Figure 1. S&T Protection Overview (Initial Review).

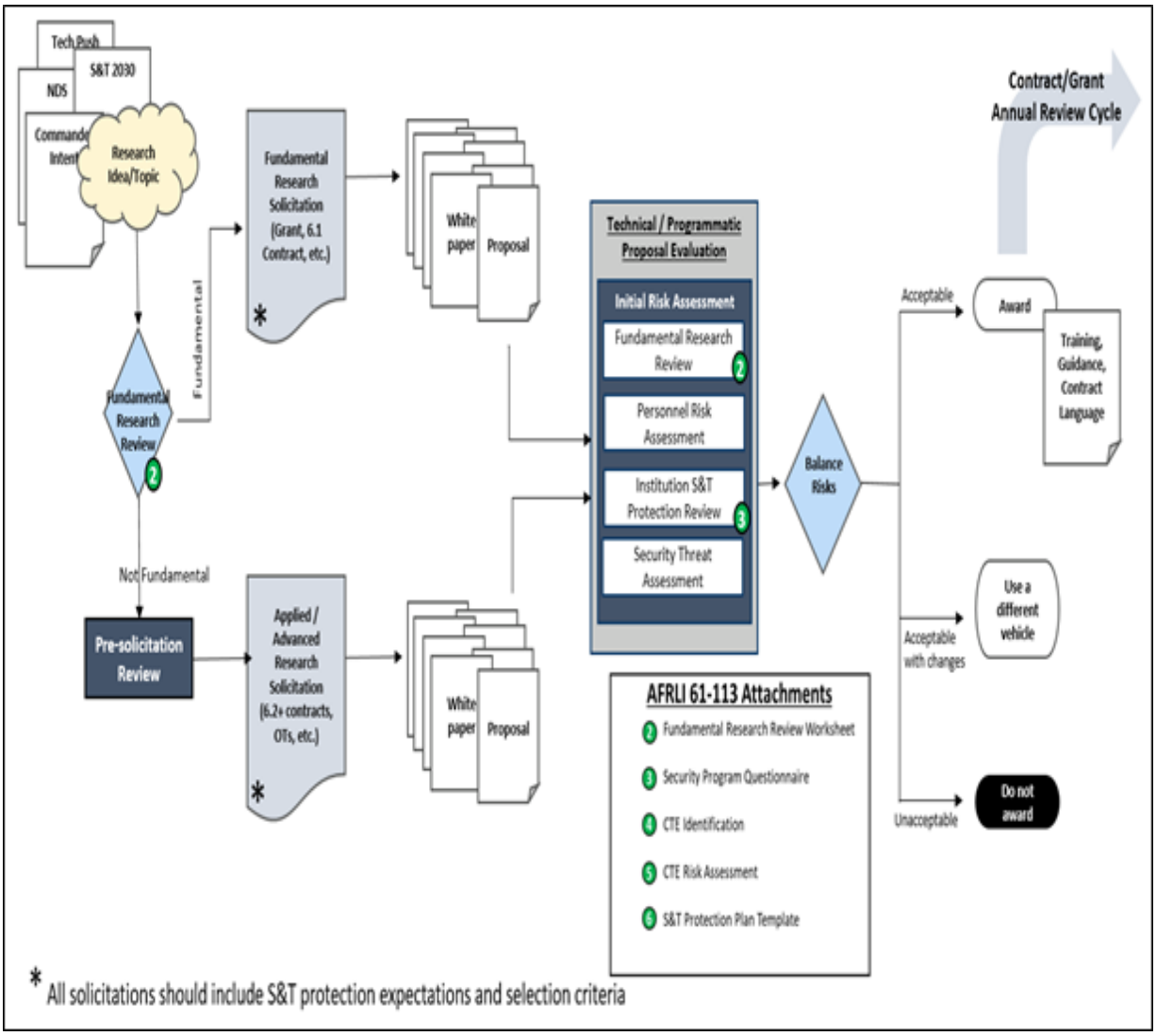
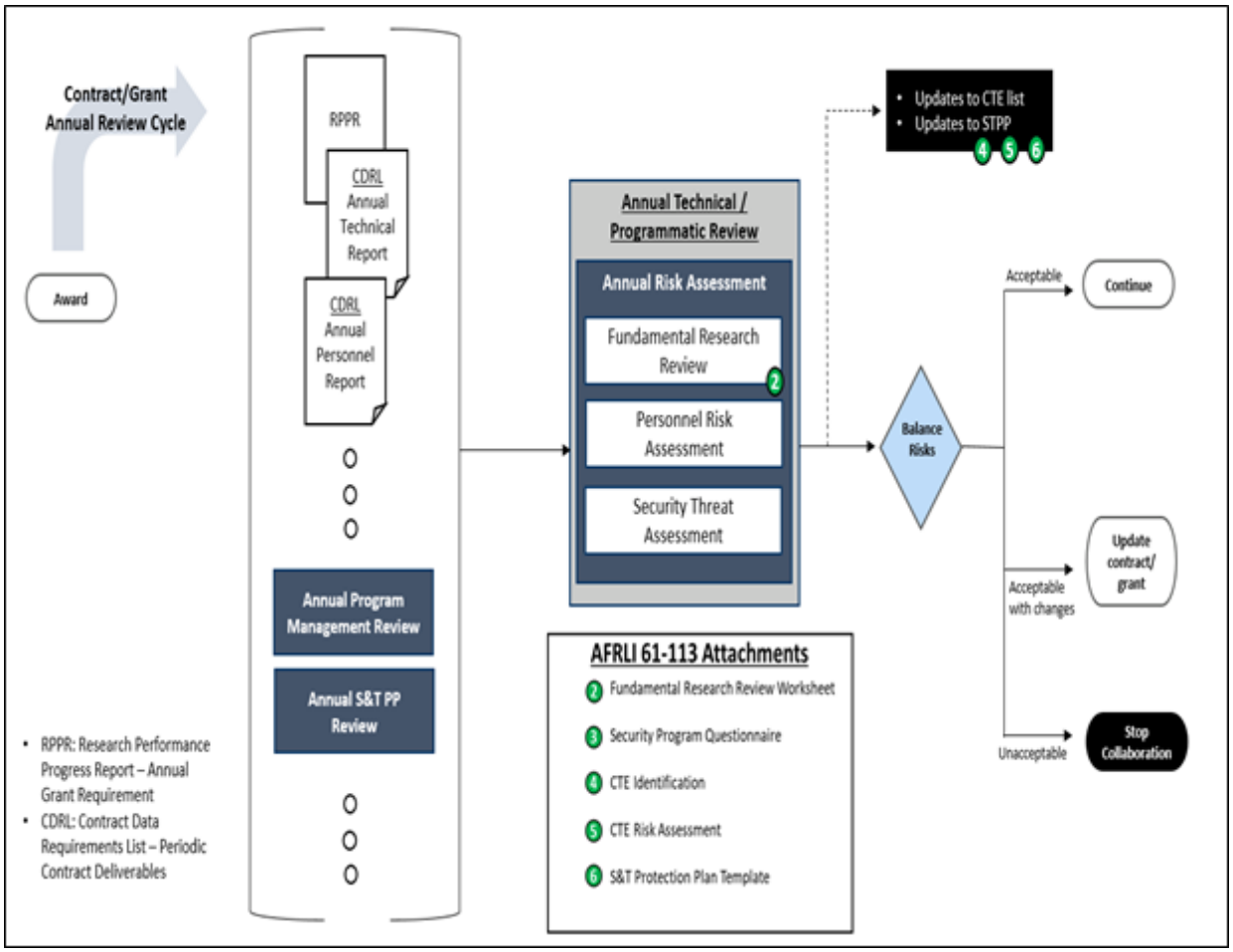


Figure 2. S&T Protection Overview (Annual Review).



3.2. **Fundamental Research Review.** The Fundamental Research Review is used to determine if an S&T effort is fundamental or if additional protection measures are required. The Fundamental Research Review Worksheet (**Attachment 2**) contains the checklist used to document this determination. This review is required prior to solicitation, during proposal evaluation, and annually thereafter for fundamental research efforts.

3.3. **Pre-solicitation Risk Review.** If an effort is determined to not be fundamental, Contracting/Agreements/Grants Officers, S&T Managers and S&T Protection Leads must review protection plans, communication plans, and/or other relevant documentation prior to solicitation release via the System for Award Management (SAM), Grants.gov, or other publicly accessible website. This review is similar to an OPSEC review and ensures compliance of any information released in the solicitation.

3.4. **Initial/Annual Risk Review.** The initial risk review is conducted pre-award as part of the proposal evaluation process. In addition to the annual technical and programmatic reviews required by AFRLI 61-108, *Management and Control of Technology Development for AFRL*, AFRL research efforts will also be reviewed for security risks annually for adversarial exploitation. The S&T Manager and S&T Protection Lead shall conduct the following:

3.4.1. **Fundamental Research Review** (Initial and Annual). The Fundamental Research Review Worksheet (**Attachment 2**) will be used to reassess all fundamental research efforts annually to ensure they have not matured beyond the fundamental research realm.

3.4.2. **Personnel Risk Assessment** (Initial and Annual). IAW the S&T effort contract, grant, or agreement, S&T Managers will review non-government research key/senior performers for workload conflicts and CoI. The SF 424, *Research and Related Senior/Key Person Profile (Expanded) Form,* and DARPA's Foreign Influence Risk Rubric, *Risk-Based Measures to Assess Potential Undue Foreign Influence Conflicts of Interest or Conflicts of Commitment*, (**https://www.darpa.mil/attachments/092021DARPACFIPRubric.pdf**) support this review, which helps identify risks of unauthorized foreign involvement in AFRL research. The Foreign Influence Risk Rubric may be used as a guide to alert S&T Managers of any concerns that should be sent to their S&T Protection Leads for further consideration. S&T Protection Leads will assess and quantify the identified risks in accordance with Msn Org policies and procedures. The S&T Protection Lead's risk assessment will be considered during the decision-making process for awarding and/or continuing the effort.

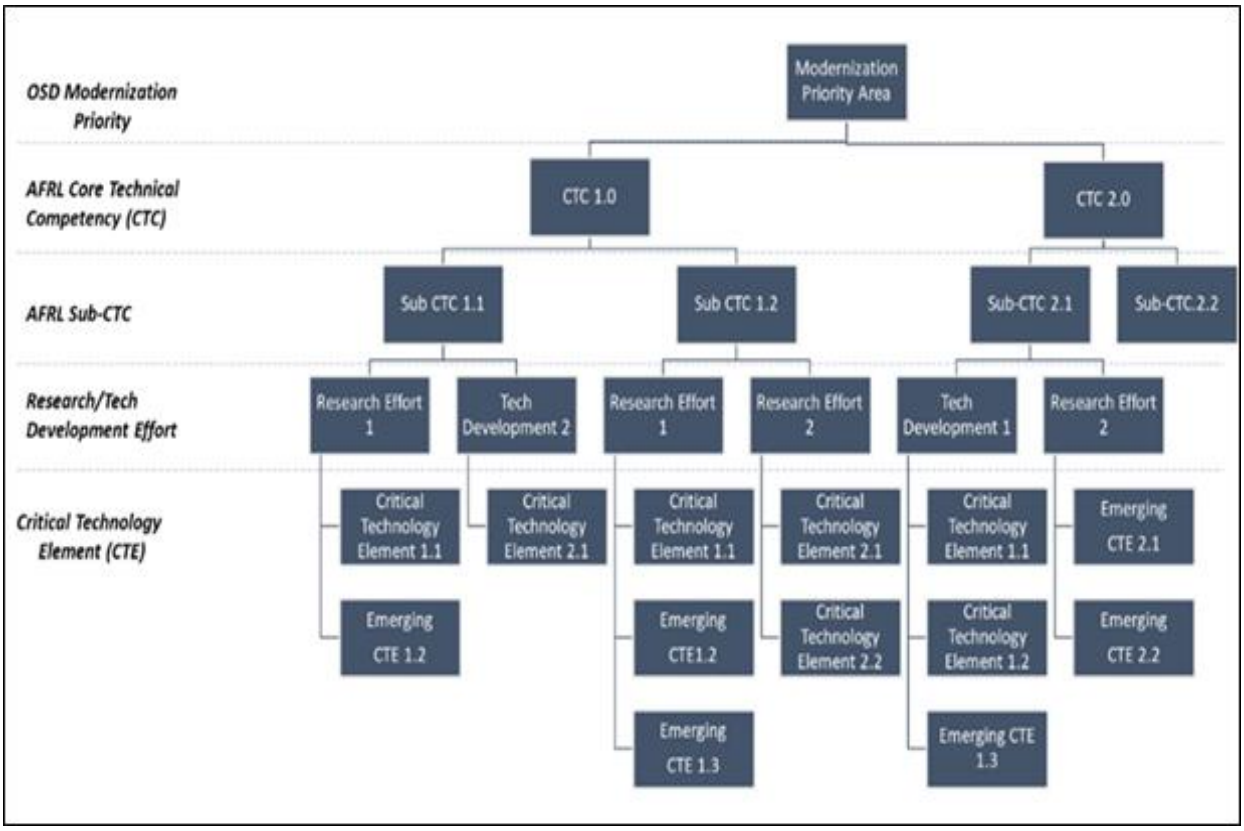
3.4.3. **Institution S&T Protection Program Review** (Initial Only). The Security Program Questionnaire (**Attachment 3**), which should be attached to any new solicitation, will be used to assess partners' security programs for potential risks. S&T Protection Leads will conduct a review of the performers' security program via information on the Security Program Questionnaire. This questionnaire is to be completed by the performers and delivered once with the proposal package.

3.4.4. **Security Risk Assessment** (Initial and Annual). Review relevant protection plans, which include, but are not limited to, CTC-level S&T Protection Plans, Customer PPPs, OUSD CP&T List, and OUSD TAPPs to ensure horizontal protection and to assess any additional risks to the effort. Provide updates as necessary.

3.5. **CTE Identification.**

3.5.1. S&T Managers must determine if there are any critical technology elements resulting from their effort. A CTE is the lowest level of information that provides a U.S. technological advantage; or is essential to the mission performance of a larger operational warfighter/support system. Efforts must be reviewed annually for new CTEs; however, S&T Managers should identify CTEs, and their required protection, as early as possible. Individuals identifying CTEs shall use a decomposition approach that leverages the established and familiar CTC structure in AFRL. Other technical organizational structures may be used with HQ AFRL concurrence. CTE must be identified one-by-one in a hierarchical approach. The hierarchy is depicted in **Figure 3**.

Figure 3. CTE decomposition strategy from OSD Modernization Priority to CTE.



3.5.2. The CTE identification process is detailed in the CTE Identification Worksheet (**Attachment 4**). The CTE Identification Worksheet provides a series of steps and questions to be considered when identifying CTE. The results from this worksheet will later be captured in the S&T Protection Plan, which serves as a means to document the elements requiring protection throughout the effort's lifecycle. When CTE is identified, an evaluation is required to determine the need for an annex to the associated CTC-level S&T Protection Plan, which contains additional protection measures.

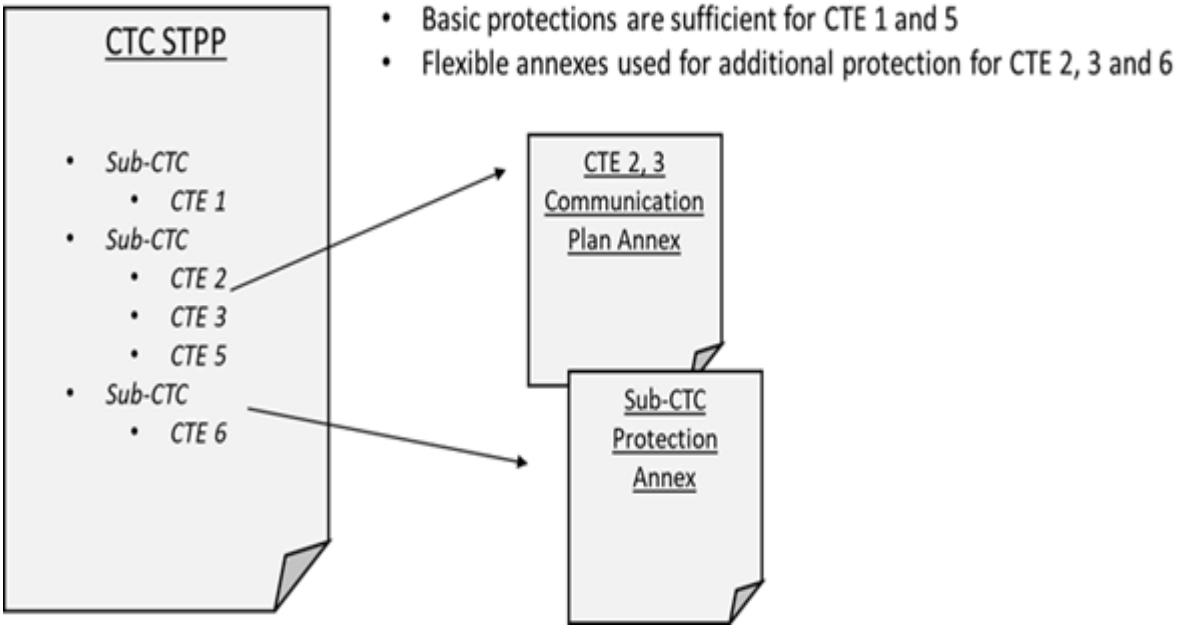
3.5.3. Msn Org S&T Protection Working Group Chairs will report Msn Org CTE lists, including the full decomposition, to HQ AFRL S&T Protection Working Group annually. This information is incorporated into the OSD CP&T list for horizontal protection across the DoD. HQ AFRL maintains the current AFRL CTE list and template on SIPRNet.

3.6. **CTE Risk Assessment.** After completing the CTE Identification Worksheet (**Attachment 4**), the S&T Managers and S&T Protection Leads will complete the CTE Risk Assessment (**Attachment 5**) to determine the risk of adversarial exploitation from the unauthorized disclosure of that information and the appropriate countermeasures. The CTE Risk Assessment will be validated annually by the S&T Manager and S&T Protection Leads to maintain awareness of emerging threats and vulnerabilities, and plan for the protection of that information throughout the effort's lifecycle. The results from the CTE Risk Assessment will be incorporated into the formal CTC-level S&T Protection Plan or effort-specific annex.

3.7. **S&T Protection Plan.**

3.7.1. AFRL Msn Orgs will use a consistent approach to develop S&T Protection Plans. S&T Protection Plans will be established for each CTC, sub-CTC, or other HQ AFRL-approved structure that contains CTE as defined above. Msn Orgs will determine the most appropriate structure to use for their S&T Protection Plans. Other structures will be approved on a case-by-case basis by the HQ AFRL S&T Protection Lead. If the S&T Manager, CTC-level S&T Protection Plan owner, and S&T Protection Lead determine that additional protection is needed for a specific effort, an annex can be created. A S&T Protection Plan annex may contain effort-specific risk assessment information, mitigation strategies, and/or communication strategies.

Figure 4. A CTC S&T Protection Plan may have several annexes to address program-specific needs.



3.7.2. The S&T Protection Plan must document, at a minimum, (1) CTEs and enabling technologies, (2) threats to and vulnerabilities of these items, and (3) selected countermeasures to mitigate associated risks. The document is intended to be iterative and flexible, allowing S&T Managers to account for changes to an effort that may result in the introduction of previously unidentified risks (e.g. the rotation of personnel with program access, new and emerging threats, required exceptions for testing and evaluation, etc.).

3.7.3. Existing PPPs as defined in AFRLI 63-113, *Program Protection Planning for the Air Force Research Laboratory*, will transition to S&T Protection Plans when they expire or are due for updates. While similar to existing PPPs, S&T Protection Plans are focused on protecting research and emerging technologies of all Technical Readiness Levels (TRL) before they transition to acquisition programs. AFRL protection information and strategies transition to customers' protection plans as technologies transition from AFRL research to customer programs.

3.7.4. Technology Area Protection Plans (TAPPs) have been established for each OSD S&T modernization priority area. The TAPPs are designed to reduce compromise or loss of critical technologies and protect against unwanted technology transfer. S&T Protection Plans will be consistent with their applicable TAPPs and all available horizontal protection guidance.

Figure 5. As technology transitions from AFRL to customers, protection transitions from S&T Protection Plan to customers' PPP

3.7.5. **Attachment 6** contains the S&T Protection Plan Template.

3.7.6. In supporting the requirements for an annual risk assessment as outlined in DoDI 5000.83, all AFRL efforts and S&T Protection Plans will be reviewed annually by the Msn Org's S&T Protection Working Group to ensure protection strategies are up to date.

3.8. **Contractual Considerations.**

3.8.1. The acquisition/assistance team, including but not limited to, contracting professionals, S&T Managers, and S&T Protection Leads will consider the following when developing solicitations and Federal Acquisition Regulation (FAR)-based contracts, grants, agreements, and OTs. Each acquisition has unique qualities and will require a tailored approach in some cases, but the practices detailed below shall be reviewed and applied as appropriate.

3.8.2. **Pre-award/Strategy Development:** During the acquisition strategy development phase, the acquisition team will work in concert with the requirement owner to review the identified S&T Protection risk areas and requirements. The acquisition team will consider the impact of the identified S&T Protection risk areas and requirements and include appropriate risk-mitigating processes in the Acquisition/Assistance Strategy Plan. These include, but are not limited to:

3.8.2.1. **Personnel Restrictions:** Develop language for the solicitation which clearly details any restrictions on contractor personnel based on any classifications made IAW 32 C.F.R. 2001. This allows contractors to make appropriate bid/no-bid decisions based on their ability to provide contractor personnel who can meet the restrictions.

3.8.2.2. **Offeror Security Program:** Require offerors to provide documentation of their Security Program Plan for initial Institution S&T Protection Program Review. This may be a pre-existing document that the offeror uses as a matter of course or a plan developed specifically for the acquisition at hand. The solicitation should specify that the purpose of requesting the plan is to evaluate the offeror's capacity for protecting the Government's S&T and that failure to demonstrate a plan adequate to meet the needs of the requirement may be grounds for considering the proposal unawardable.

3.8.2.3. **Evaluation Criteria:** The acquisition team may establish evaluation criteria specific to S&T Protection. This may include consideration of S&T Protection in an offeror's past performance, or the requirement of the contractor to address S&T Protection in its proposal based on a requirement of the Statement of Work (SOW) or other similar document. In all cases, the evaluation criteria must be relevant to the requirement and be clearly defined for the offerors.

3.8.2.4. **S&T Protection Deliverables:** When deemed appropriate, the acquisition team may establish a Contract Data Requirements List (CDRL), which requires that the awardee provide an initial report of all personnel at award, a report for any new personnel who join the contract, agreement, grant, or OT, and an annual report of contractor personnel providing support. Utilization of the SF 424, *Research and Related Senior/Key Person Profile (Expanded) Form*, is recommended when establishing this requirement. The purpose of this report is oversight and should not be construed as relieving the contractor of any S&T Protection requirements within the contract, grant, agreement, or OT.

3.8.3. **Post-award/Administration:** After award, the acquisition team's responsibility to S&T Protection continues. Regular surveillance of the contract, grant, agreement, or OT from an S&T Protection perspective should be appropriately tailored to the requirement. The acquisition team may choose to include post award surveillance of the contractor's S&T Protection program and processes as a part of a Quality Assurance Surveillance Plan (QASP) or a document of similar purpose. This will provide the acquisition team with a standard process for surveilling and documenting contractor performance against S&T Protection requirements and prescribe contractual remedies for any violations.

HEATHER L. PRINGLE
Major General, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*, 20 July 2020

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

National Security *Presidential Memorandum (NSPM) 33*, 14 January 2021

OUSD(R&E) *Science and Technology (S&T) Protection Guide*, 31 March 2021

National Security *Decision Directive (NSDD) 189*, 21 September 1985

Prescribed Forms

None

Adopted Forms

SF 424, *Research and Related Senior/Key Person Profile (Expanded) Form*

DD Form 254 *Contract Security Classification Specification*, December 1999

AF Form 847, *Recommendation for Change of Publication*, 22 September 2009

Abbreviations and Acronyms

A&A—Assessment and Authorization

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigation

AFRIMS—Air Force Records Information Management System

AFRL—Air Force Research Laboratory

AFRLI—Air Force Research Laboratory Instruction

BAA—Broad Area Announcement

CDRL—Contract Data Requirements List

CI—Counterintelligence

CoC—Conflict of Commitment

CoI—Conflict of Interest

CPI—Critical Program Information

CP&T—Critical Programs and Technologies

CTC—Core Technical Competency

CTE—Critical Technology Element

CUI—Controlled Unclassified Information

DoD—Department of Defense

DoDI—Department of Defense Instruction

FAR—Federal Acquisition Regulation

FDO—Foreign Disclosure Officers

HQ—Headquarters

ISSM—Information System Security Manager

ISSO—Information Security Officer

ITA—Integrated Threat Assessment

ITAR—International Traffic in Arms Regulations

Msn Org—Mission Organization

NDS—National Defense Strategy

OPR—Office of Primary Responsibility

OPSEC—Operations Security

OSD—Office of Secretary of Defense

OT—Other Transaction

OUSD (R&E)—Office of Under Secretary of Defense (Research and Engineering)

PPP—Program Protection Plan

QASP—Quality Assurance Surveillance Plan

RDS—Records Disposition Schedule

R&D—Research and Development

RMF—Risk Management Framework

RPPR—Research Performance Progress Report

S&T—Science and Technology

SAM—System for Award Management

SAP—Special Access Programs

SCG—Security Classification Guide

SCI—Sensitive Compartmented Information

SOW—Statement of Work

SIPRNet—Secure Internet Protocol Router Network

TAPP—Technology Area Protection Plan

TRL—Technology Readiness Level

Terms

Conflict of Commitment (CoC)—A conflict of commitment is a situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many institutional policies define conflicts of commitment as conflicting commitments of time and effort, including obligations to dedicate time in excess of institutional or funding agency policies or commitments. Other types of conflicting obligations, including obligations to improperly share information with, or withhold information from, an employer or funding agency, can also threaten research security and integrity, and are an element of a broader concept of conflicts of commitment.

Conflict of Interest (CoI)—A conflict of interest is a situation in which an individual, or the individual's spouse or dependent children, has a financial interest or financial relationship that could directly and significantly affect the design, conduct, reporting, or funding of research.

Core Technical Competency (CTC)—Represent the technical foundation that is difficult to duplicate and allows AFRL to provide unique technical leadership. CTCs span basic research, applied research, and advanced technology development. CTCs are the people, information, facilities, equipment, and programs that allow AFRL to solve critical Air Force and national security problems.

Critical Technology—Sensitive technical data, concepts, hardware, software, processes, know-how, design details, scientific information, research results, and capability elements that are essential to (or reveal) the design, research, development, production, operation, application, performance, or maintenance of an article, capability, or service that significantly contributes to a current or future U.S. technological, competitive, or lethal advantage over a foreign adversary capability, whose acquisition by potential adversaries would prove detrimental to the national security of the United States.

Critical Technology Element (CTE)—The lowest level of information that makes a technology unique and provides a technological advantage, or is essential to the mission performance of a larger operational warfighter/support system.

Fundamental Research—Basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

Horizontal Protection—Process to ensure protective countermeasures addressing the risk of possible loss or compromise for the same or similar CTE associated with more than one effort, program, component, system, or subsystem have been evaluated and risk accepted, or mitigated by affected entities. Horizontal protection ensures that an investment made by one program/project to mitigate the risk of CTE compromise is not diminished or wasted due to another program exposing the same or similar CTE to much greater risk.

Mission Organization—Those organizations in AFRL that are executing the scientific and medical mission of AFRL. AFOSR, AFRL/RD, RG, RI, RQ, RS, RV, RW, RX, RY, STO and the 711 HPW, and any new organization established to execute scientific and medical technology missions.

Technology Area Protection Plan (TAPP)—An OSD document that adapts and applies principles of program protection planning to each S&T Modernization Priority Area. TAPPs provide a decomposition of each modernization area into its critical sub-elements and enabling technologies, define technical thresholds that require protection, offer communication guidance, and suggest Department- and program-level risk mitigations to help consistently protect emerging and existing DoD S&T investments at conception and throughout the program lifecycle. TAPP appendices include known contracts and grants; DoD programs and research programs; classification guides; international agreements; vendors, research centers, and companies relevant to the Modernization Priority Area.

Attachment 2

FUNDAMENTAL RESEARCH REVIEW WORKSHEET

Table A2.1. Fundamental Research Review Worksheet.

Objective: The Fundamental Research Review is conducted to determine whether an effort contains elements that may be pursued openly without restriction IAW NSDD 189. **Intended User/Audience:** S&T Managers in coordination with S&T Protection Leads and CI Representatives, as required. **FUNDAMENTAL RESEARCH REVIEW QUESTIONS:** The scope and results of the contract, grant, agreement or other transaction authority is most likely fundamental research when the responses to the following statements are TRUE:		
The effort is most likely fundamental research if:	**True or False**	**Comment**
1. It would ordinarily be published and shared broadly within the scientific community without restrictions.		
2. It will NOT have a negative impact on national security when disclosed in the public domain, or combined with other available public domain information.		
3. It is NOT covered in the International Traffic in Arms Regulations (ITAR) (i.e., enumerated on the U.S. Munitions List) or listed on the Export Administration Regulations' Commerce Control List (CCL) (e.g., listed with an Export Control Classification Number (ECCN)).		
4. It will NOT contain proprietary research from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.		
5. It does NOT require classification consistent with EO 13526, "Classified National Security Information."		
6. It does NOT involve disclosing performance characteristics of military systems or national intelligence or unique development, manufacturing, assembly, testing, operation, maintenance, or repair processes that are critical to defense.		
7. It does NOT require access to controlled unclassified or classified information to support the conduct of the research.		
8. Unauthorized disclosure of information related to this research effort would NOT cause damage to National Security.		

If ALL answers are TRUE, then STOP. This review is complete and the research effort and related technologies can safely be considered fundamental.

If ANY answers are FALSE, the research effort requires a more in-depth review to determine if the research effort and related technologies can be considered fundamental. Please contact your S&T Protection Lead.

Attachment 3

SECURITY PROGRAM QUESTIONNAIRE

Figure A3.1. Security Program Questionnaire.

Objective: This questionnaire is used to review the security program and practices of the institutions receiving research funding.
Intended Audience/User: Completed by collaborators; reviewed by S&T Protection Lead.

Date Submitted: _____

Applicant Name: _____

Cage Code/SCL and level *(if applicable):* _____

Completed by Name: _____

Position/Title: _____

1. What are your physical security plans?

2. What information security processes are in place?

3. Where will information for this effort be stored? (*examples: computers, cloud, file cabinets, etc.*)

4. What procedures are in place for transmission/transportation of information for this effort?

5. What procedures are in place for disposal and destruction of information for this effort?

6. What procedures are in place for reproduction of information for this effort?

7. What safeguards are in place for personnel who can access information for this effort?

8. What is the plan for safeguarding GFE/GFI?

9. What procedures are in place for cybersecurity or network protection?

10. What operations security processes are in place to prevent adversaries' access to information for this effort or actions that would compromise your projects?

11. What processes are in place to deter, detect, and mitigate actions of insider threat?

12. What procedures are in place to handle if information for this effort is compromised?

13. Are you willing to provide AFRL S&T Protection training to all personnel with access annually?

Additional comments:

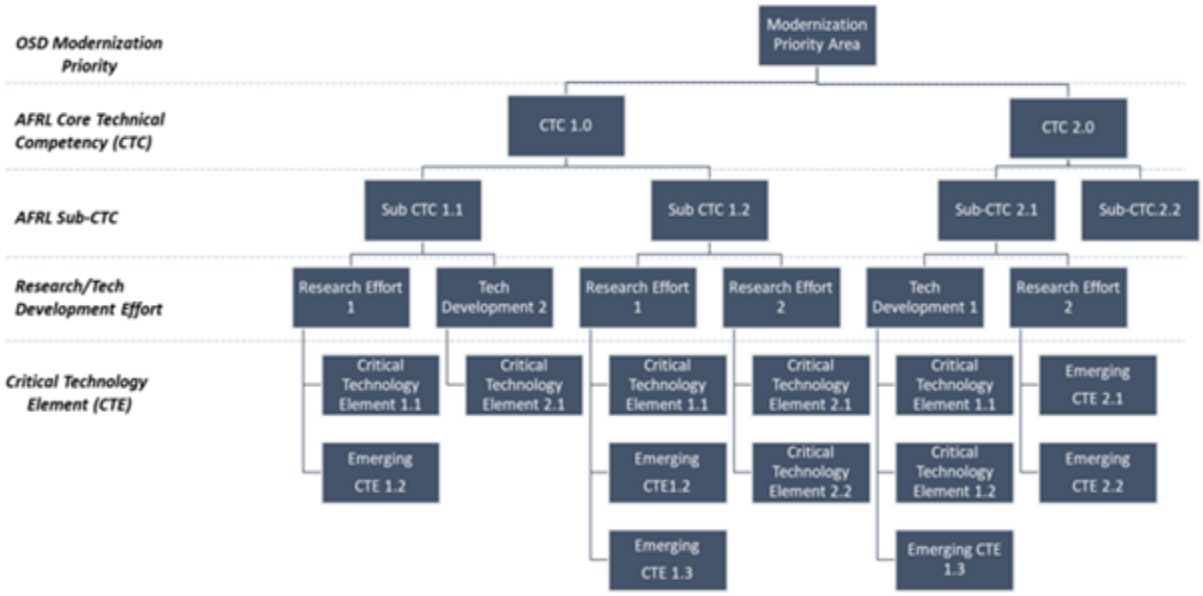
Attachment 4

CRITICAL TECHNOLOGY ELEMENT (CTE) IDENTIFICATION

Figure A4.1. Critical Technology Element (CTE) Identification.

Objective: Provide a methodology to decompose an effort into individual technology elements and to determine which of those elements are CTEs. A virtual tool for completing the technical decomposition and CTE identification described below is available at AFRL/DSI SharePoint site (https://usaf.dps.mil/teams/10722/InfoPro/SitePages/Science%20and%20Technology.aspx). This attachment may be used to facilitate teams' efforts for CTE identification.

Intended user/audience: S&T Manager and technical team in coordination with security team.



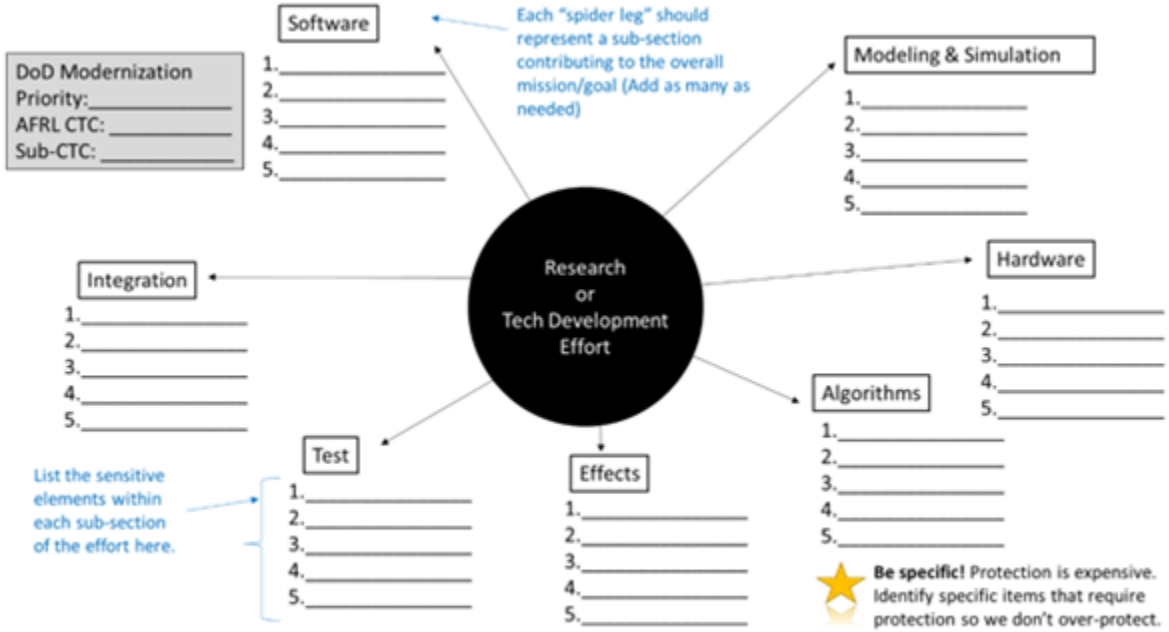
Step 1: Document the DoD Modernization Priority Area, AFRL Core Technical Competency (CTC), and Sub-CTC, or other HQ AFRL-approved structures, for the research/technology development effort on the example Spider Chart.

Step 2: Document the research or technology development effort in the center of the example Spider Chart. While technology program names/acronyms may be included for reference, please also include a description of what the effort is doing. This description should be useful for cross-service horizontal protection. For example:

- **Cannot horizontally protect:** Project RoCKInG ChAir
- **Can horizontally protect:** Restful sitting devices for post-retirement individuals

Step 3: Identify all sensitive elements for the effort. This may include, but is not limited to, hardware, software, test equipment, integration techniques, etc. Be sure to drill down to the lowest level of unique element that requires protection to prevent over-protecting. Use the example Spider Chart to document all sensitive elements.

Spider Chart



Step 4: For each of the sensitive elements identified in Step 3, one element at a time, answer the following questions to determine if that element is CTE. (Note: an answer of "Yes" to any of the questions may indicate that the element is CTE):

1. Is it unique, emerging, disruptive, game-changing, novel, exclusive, and/or state-of-the-art (or will it be after maturation)?

2. Does it significantly contribute to a U.S. technological, competitive, or lethal advantage over a foreign adversary capability?

3. Does it make a significant contribution to the military capability of another country or combination of countries that would be detrimental to the U.S.?

4. Was it previously identified as a critical technology, component(s), system, or platform by another program or service (reference appropriate TAPP, PPP, etc.)?

5. Is it science or a technology that might be expected to create an advantage over our strategic competitors?

6. Is it design and manufacturing know-how, technical data, keystone equipment, novel or unique materials, and inspection and test equipment?

7. Is it software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment?

8. Is it military-unique datasets for training algorithms or AI?

9. Is it information about applications, capabilities, performance characteristics, fragile analytic processes or techniques, processes, and end-items?

10. Is it elements or components essential to a military system or network mission effectiveness?

11. Does it involve a method, technique, application, or production process that is unique to the U.S. Government and/or industry?

12. Does it involve a method, technique, application, or production process that cannot or should not be achieved using alternate methods and techniques?

13. Does it involve a method, technique, application, or production process that is essential to system capability and performance?

Step 5: For each CTE identified in Step 4, document if/how the CTE is currently being protected. Is it currently or will it be included in an S&T Protection Plan, Program Protection Plan, etc.?

Attachment 5

CRITICAL TECHNOLOGY ELEMENT (CTE) RISK ASSESSMENT

Figure A5.1. Critical Technology Element (CTE) Risk Assessment.

Objective: This CTE Risk Assessment is used to determine the risk associated with the unauthorized disclosure of that information.
Intended user/audience: S&T Manager and S&T Protection Leads

Step 1: Document all CTE identified from the Attachment 4: CTE Identification.

Step 2: For each of the CTE identified listed, one element at a time, answer the following questions to identify emerging threats and vulnerabilities or to maintain awareness of any existing threats and vulnerabilities, and plan for the protection of that information throughout the effort's lifecycle.

1. Is the CTE Organic (originated by owning organization) or Inherited (owned by another organization)?

2. Will loss/compromise/unauthorized disclosure of the CTE result in Total (T) compromise of mission capability of the technology, or Unacceptable (U) compromise of mission capability or significant mission degradation?

3. Is the CTE or associated information Classified or CUI? **NOTE: If loss of the information could cause damage to national security, STOP, and contact your S&T Protection Lead for guidance on the classification process.**

4. What are the applicable Distribution/Dissemination Statements?

5. Do any of the below apply:

a. DoD Modernization Priorities

b. List of Critical Programs and Technologies for Prioritized Protection

c. OUSD(R&E) Technology Area Protection Plans (TAPPs)

d. Service/Agency Priorities

f. Other Applicable Priorities

6. Does the CTE have applications across multiple domains or priorities?

7. Does the CTE contain export control information?

8. Does this technology fall under an existing Program/S&T Protection Plan?

9. Have the technologies been identified for transition or does the technology have strong potential to transition out of the directorate to an activity ready to assume program management responsibility due to underlying value/advancement of warfighter capability?

10. Are there any known vulnerabilities of this technology that if divulged would result in release of sensitive information or cause OPSEC concerns, a public outcry of diplomatic harm, or allow an adversary or foreign country to copy, counter, or defeat the technology?

11. Is there requested or required foreign access?

12. What is the Technology Readiness Level?

13. Does the research effort include a technology element or area tied to the interest of specific state actor?

14. Would the loss, theft, or compromise of information related to critical technology elements or enabling technologies likely result in foreign adversaries filling critical technology gaps?

15. Would the unauthorized disclosure of CUI elements likely result in foreign adversaries filling critical technology gaps?

16. Would the loss, theft, or compromise of classified information likely result in foreign adversaries filling critical technology gaps?

17. What plan is in place to maintain awareness of emerging threats and vulnerabilities?

18. How will emerging threats and vulnerabilities be integrated into the existing plan?

Step 3: Determine if countermeasures are necessary for protection of your identified CTE from the following Countermeasures Groups:

Countermeasure Groups

1	Information Security	9	Supply Chain Risk Management	17	Control Guide
2	Personnel Security	10	Cyber Security	18	Intelligence Activities
3	Industrial Security	11	Defense Exportability Features	19	Foreign Investment
4	Physical Security	12	Anti-Tamper	20	SCG
5	Operations Security	13	Foreign Disclosure	21	Program/S&T Protection Plan
6	Training	14	Contracting	22	Technology Area Protection Plan
7	Hardware Assurance	15	Counterintelligence Support Plan	23	Other
8	Software Assurance	16	Export Control		

List identified CTE and annotate if the Countermeasures Group needs to be implemented, has protection inherited from other organizations, or are not applicable.

	List all CTE from Sheet 1	Annotate Below: **X**=Implement; **I**= Protection Inherited from other Org; **N/A**= Not applicable																					
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**
1	(Example) Source Code	x	x	N/A	x	x	x	x	x	x	x	N/A	N/A	x	N/A	x	N/A	x	x	N/A	x	x	I	I
2																								
3																								
4																								
5																								
6																								

Step 4: Provide explanations of countermeasures. Continue to complete updates as technology matures/changes, and/or upon update of Integrated Threat Assessment.

Step 5: The results from the CTE Risk Assessment will be incorporated into the formal CTC-level S&T Protection Plan or effort-specific annex.

Attachment 6

OUSD S&T PROTECTION PLAN TEMPLATE

Figure A6.1. OUSD S&T Protection Plan Template.

S&T Protection Plan Update Record

Revision Number	Date	Changes	Approved By

Contents

1. Introduction, Updates, and Responsible POCs

1.1. 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.

1.2. 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	

1.3. 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			

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 managers and CI Representatives 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 2.1. 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 Managers and CI Representatives 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. 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. 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. 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. 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. 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. 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. 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. 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

Enter Text Here

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

4.7. 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. 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. 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. 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. 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. 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. 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.