| 미국편 |

국제공동연구 연구보안

길잡이

2025.7.

과학기술정보통신부
Ministry of Science and ICT

KISTEP 한국과학기술기획평가원
Korea Institute of S&T Evaluation and Planning

| 미국편 | 국제공동연구 연구보안 길잡이

CONTENTS

요 약 문

미국의 연구보안 제도·규정 개요

- (개요) 미국 정부는 미국 자금이 투입된 연구 활동의 보안을 강화하기 위해 다양한 조치를 시행하고 있으며, 이에 따라 우리나라 연구자들도 미국의 연구자금 수혜 및 국제공동연구 수행 시 관련 보안 규정을 이해하고 유의할 필요

- (관련 법령 및 규정) 미국의 주요 연구보안 정책은 다음의 상위 법령 및 지침에 기반
  - 「국가안보대통령교서-33 (NSPM-33)」
  - OSTP의 NSPM-33 연방기관 이행지침
  - 2022년「CHIPS 및 과학법」

- (주요 기관) 미국 의회조사국(CRS)에 따르면, 2025 회계연도(FY2025) 기준 주요 R&D 자금 지원기관은 전체 연방 연구개발 예산의 약 92.5%를 차지하며, 구체적으로는 국방부(DoD, 41.8%), 보건복지부(HHS, 27.1%), 에너지부(DOE, 11.6%), NASA(8.5%), 국립과학재단(NSF, 3.5%) 순임

- (공통 보고 의무) 모든 연방 자금 수혜 연구자들 중 연구책임자 등 '대상 인물'은 악성 외국 인재채용프로그램(MFTRP)에 현재 참여하고 있지 않음을 확인하고, 모든 외국 인재채용 프로그램(FTRP) 참여 이력을 공개해야 함

1 에너지부(DOE)

- (개요) 미국 에너지부(DOE)는 개방형 국제협력 정책과 함께 연구보안 강화를 위한 체계적 제도를 운영 중이며, 기술 민감도, 연구자의 외국 연계 여부, 국익과의 정합성을 기준으로 국제공동연구 승인 여부를 평가

- (관련 규정) 미국의 주요 연구보안 정책은 다음의 상위 법령 및 지침을 기반으로 함
  - 외국정부 활동 : DOE O 486.1A
  - 외국인 접근 : DOE O 142.3B
  - 협동연구개발계약(CRADA) : DOE O 483.1B
  - 전략적 파트너십(SPP) : DOE O 481.1E
  - 국립연구소 교류지침 : DOE P 485.1A
  - 공식 외국출장 : DOE O 550.1
  - 기술 민감도 분류기준 : S&T Risk Matrix

① (DOE O 486.1A) Foreign Government Sponsored or Affiliated Activities

  - DOE 직원 및 Contractor Personnel의 위험국가 관련 외국 정부 후원 인재 프로그램(FGTRP) 참여 금지
  - DOE와 고용 관계가 있는 직원 및 계약자의 위험국가 관련 기타 외국 정부 연계 활동(자금 수령, 직위 수락 등)은 DOE 장관 또는 고위 승인자 사전 승인 필요

② (DOE O 142.3B) Unclassified Foreign National Access Program

- 외국인은 FACTS 시스템 등록, 이력서 제출, 신분 확인 등 절차 필요
- Red 기술 접근 시 위험국가 국적자는 강화된 승인 및 CI 심사 필요

③ (DOE O 550.1 Chg 1) Official Travel

- (DOE 직원 준수 사항) DOE 직원 및 계약자의 모든 공식 해외 출장은 FTMS 시스템 등록 및 사전 승인 필요하며, 민감국가 대상지 방문 또는 민감 주제 포함 시 IN 사전 브리핑 필수

④ (S&T Risk Matrix) Science & Technology Risk Matrix

- 기술 민감도를 Red/Yellow/Green으로 분류
- Red는 제한기술로 간주되어 위험국가 접근 시 본부·현장 심사 및 승인이 필수

⑤ (DOE P 485.1A) Foreign Engagements with DOE National Laboratories

- 모든 외국기관 협력은 DOE 본부 사전검토 대상
- MOU, LOI, SPP, CRADA 등 포괄적 검토 범위

⑥ (DOE O 483.1B Chg 2) Cooperative Research and Development Agreements (CRADA)

- 미국 내 기술 활용 우선, FOCI 심사, IP 분배 조건 충족 필요
- 위험국가 또는 Red 기술 관련 협력은 DOE 차관 승인 필수

⑦ (DOE O 481.1E Chg 1) Strategic Partnership Projects (SPP)

- DOE/NNSA 미션과 정합성, 산업경쟁 저해 여부, 리소스 낭비 방지 등 요건 검토
- Red 기술 포함 시 FOAB·DOE 차관 면제 승인 필수

〈참고〉 DOE의 위험국가(Countries of Risk) 및 민감국가(Sensitive Countries) 관련 조치

» (개요) 미국 에너지부(DOE)는 지정된 위험국가 및 민감국가와의 연구 협력, 기술 접근, 인력 교류에 대해 다양한 사전 승인 및 통제조치를 운영하고 있으며, 관련 규정은 국가안보, 기술보호, 방첩 활동 등과 연계되어 있음

① 위험국가 관련 조치

- (정의) 국가정보국의 위협 평가 및 국가 방첩 전략에 따라 DOE 차관이 지정
- (현재 지정국) 중국, 러시아, 이란, 북한, 벨라루스 (2025년 5월 기준)이며, 변동 가능
- 관련 규정 및 주요 조치
  - (제한기술 접근 통제) 위험국가 국적자/기관의 Red 등급 기술 접근 시 DOE 본부 및 현장 승인 필수
  - (인재유치 프로그램 제한) DOE 직원 및 계약자 대상 위험국가 FGTRP 참여 금지, 기타 외국 정부 연계 활동 제한
  - (국립연구소 협력 제한) 위험국가와 Red 기술 협력(MOU, CRADA, SPP 등) 금지, 사전 면제 필요
  - (CRADA 체결 제한) Red 기술 포함된 CRADA 협력 시 FOAB 및 DOE 차관 예외 승인 필요
  - (SPP 체결 제한) Red 기술 포함된 SPP 협력 시 FOAB 및 DOE 차관 예외 승인 필요

② 민감국가 관련 조치

- (정의) 국가안보, 핵 비확산, 경제안보, 테러지원 등을 고려해 정책적으로 지정
- (현재 지정국) 외부 비공개, DOE 내부 SCL(Sensitive Countries List)로 관리
- (제한 여부) 국제과학협력, 일반적 접촉, 출장 등을 금지하지 않음
- 관련 규정 및 주요 조치
  - (국립연구소 협력 사전 평가) 민감국가 국적자 연구자와의 협력 시 접근 가능 여부를 사전 검토
  - (CRADA 협력 정보 보고) 계약기관이 민감국가와 수익·계약관계 시 FOCI 심사 대상, 완화조치 필요
  - (기술 및 시설 접근 제한) 민감국가 국적자의 NNSA 접근 시 인덱스 조회 필수, 기록은 FACTS에 등록
  - (방첩 브리핑 (출장 시)) 민감국가 출장 또는 접촉 시 방첩 브리핑 수행
  - (비공식 민감국가 여행) 민감국가 여행 전·후 보고 및 브리핑, 가족 거주 시 3일 이내 보고
  - (방첩 프로그램 평가 항목) 민감국가 인물 접촉 기록의 정확성·시의성 등 방첩 성과 평가 항목 포함

2 국립과학재단(NSF)

» (개요) NSF는 외국 영향, 이해충돌, 중복자금 수혜 방지를 위해 연구보안 규정을 지속 강화 중이며, 「CHIPS 및 과학법」에 따라 연구보안 전담 조직을 운영함. 국무부가 지정한 우려국가(중국, 러시아, 이란, 북한 등)와의 협력은 강화된 심사 대상

» (주요 연구보안 규정 및 의무 사항) 2024년 5월 20일 개정된 PAPPG 24-1 기준으로 다음 사항 공개·보고 의무화됨

- (외국 자금-Current & Pending Support) 외국 정부·기관의 직접/간접 지원 (연구비, 장비, 인력 등)
- (외국 무보수 기여-Current & Pending Support) 외국 기관의 현물(in-kind) 기여, 무보수 공동연구 포함
- (외국 직위-Biosketch) 외국 기관과의 모든 임용·자문·방문 연구 등 (보수 여부 무관)
- (외국 협력자-COA) 최근 48개월 내 공동연구자, 공동저자, 지도교수·제자 관계 등

» (MFTRP 금지 및 인증) 모든 주요 인력은 제안서 제출 시점부터 MFTRP(악성 외국 인재유치 프로그램) 불참을 개별 인증해야 함

» (기관 요건 : 연구보안계획 자체 인증) 연간 NSF 수혜액이 $500,000 이상인 기관은 자체 연구보안계획을 인증해야 함

» (규정 위반 시 조치) 누락 기재, 허위 기재, MFTRP 허위 인증 시 관련 규정에 따라 조치

3 국립보건원(NIH)

» (개요) 미국 내 생물의학 연구의 무결성 보호를 위해 연구자 및 기관이 외국 활동, 자원, 재정 이해관계를 투명하게 공개하도록 요구

» 주요 요구사항

- (Other Support) 외국 자금, 인력, 장비 등 모든 현물 기여 포함

- (Foreign Components) 외국에서 수행되는 연구 또는 외국 소속 연구자 관여 시 NIH 사전 승인 필요
- (FCOI (재정적 이해충돌)) 외국 기관에서 발생한 금전적 이익은 소속 기관을 통해 NIH에 보고

» 보고 방식

- (Other Support) JIT 단계 및 RPPR 보고
- (Foreign Components) 최초 제안 또는 변경 시 사전 승인
- (FCOI (재정적 이해충돌)) 연 1회 이상 기관 평가 및 NIH 보고

4 항공우주국(NASA)

» (개요) GCAM(Grant and Cooperative Agreement Manual)을 통해 연구보안, 수출통제, 외국 참여자 관리 등 명확히 규정

» 주요 요구사항

- (Export Control) 외국 참여자는 수출통제법(ITAR, EAR) 적용 대상 여부 평가 필요
- (MFTRP 금지) PI, Co-PI, Co-I(연간 10% 이상 참여자)는 MFTRP 미참여를 매년 자가 인증
- (Foreign Participation Disclosure) 소속 및 역할 등 관련 정보 공개 필요

5 국방부(DoD)

» (개요) 기초연구 단계에서부터 외국 영향과 기술 유출 방지를 위해 MFTRP 금지, 정보공개, 보안심사 제도를 운영함

» 주요 요구사항

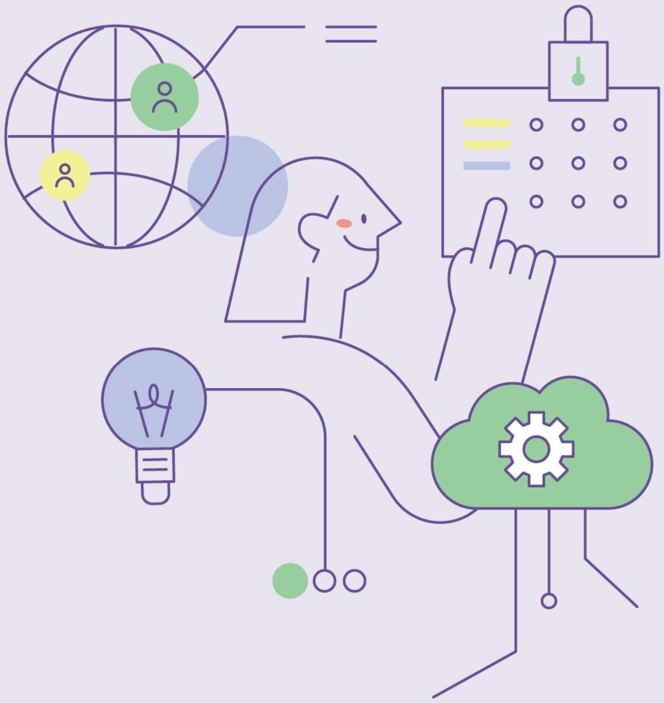
- (Current and Pending Support) 연구자의 모든 과제 및 외국 자금, 시간 투입, 수혜기관 정보 제출 의무
- (MFTRP 금지) 2024.8.9 이후 MFTRP 참여자 포함 과제 또는 관련 정책 미보유 기관은 연구비 수혜 불가
- (Security Review) 외국 영향에 대한 위험기반 심사 도입 (FTRP, FCOC 자금, 특허, BIS 등재기관 관련성 평가)

» 보안심사 결과 유형

- (Prohibited) 수혜 불가
- (Mitigation) 보완조치 조건부 수혜
- (Disclosure Only) 정보 제공만 요구
- (No Action) 문제 없음

» (이행 조치) MFTRP 참여 사실은 연례 RPPR 보고하며, 보안심사 거절 시 서면 통보 및 이의제기 절차 존재

제1장



길잡이 개요

제1장. 길잡이 개요

추진배경

- 과학기술의 글로벌화에 따라 국제공동연구는 국가 간 기술 협력과 혁신 촉진을 위한 필수적인 요소로 자리 잡고 있음
  - 우리나라는 해외 주요국들과의 국제공동연구에 적극적으로 참여하고 있으며, 이에 따라 국제공동연구 시 우리나라 연구자들이 유의해야 할 연구보안 이슈가 점점 더 중요해지고 있음
  - 국제공동연구에서는 연구보안 관련 법제 및 절차가 국가별로 상이하며, 일부 국가에서는 외국 연구자의 자금 수령, 인력 참여, 정보 접근에 대해 엄격한 규정과 의무적 공개 요건을 요구하고 있음
  - 따라서 국제공동연구에 참여하는 우리나라 연구자들은 과제 참여 초기 단계부터 각국의 연구보안 규정을 면밀히 검토하고, 정보 공개 및 이해충돌 관리 등에 대한 인식 제고를 통해 해당 규정 준수를 위한 사전적 노력 필요

목적 및 필요성

- 우리나라 연구자들이 국제공동연구 수행 시 준수해야 할 연구보안 규정을 체계적으로 정리하고, 실제 협력 과정에서 발생할 수 있는 주요 이슈 및 사례를 제시함으로써 보안 규정에 대한 인식을 제고하고 준수 역량을 높이는 데 목적이 있음
- 아울러, 가상 사례와 FAQ 형식의 실무 자료를 함께 제시함으로써, 단순한 규정 요약이 아닌 현장 중심의 실질적 가이드라인 제공을 목표로 함

주요 내용 및 구성

- (제2장) 국제공동연구의 기본 개념과 유형, 그리고 연구보안의 국제적 논의 동향 및 국내 주요 제도 소개
- (제3장) **미국 연방 R&D 예산 상위 5개 기관***(DoD, DOE, NIH, NASA, NSF)을 중심으로, 각 기관별로 상이한 연구보안 요구사항과 준수 절차를 세부적으로 분석하고, 정보 공개 의무, 외국 인재 프로그램 관련 제한, 민감기술 관리 등 우리나라 연구자 입장에서 유의해야 할 사항을 정리함

  * DoD, HHS(NIH로 대체), DOE, NASA, NSF 등

  - 이를 위해 FY2025 미국 연방 R&D 예산 요청 기준 상위 5개 기관을 중심으로, 각 기관별 연구보안 정책의 주요 내용을 분석하고, 연구자들이 사전 검토하고 대비해야 할 규정과 절차 등을 정리함
- (제4장) 현행 규정 등을 바탕으로 실제로 발생 가능한 연구보안 가상 사례들을 제시하였으며, 특히 각 사례별로 적용 규정, 연구보안 이슈, 가능한 후속 조치, 유의사항 등을 포함하여 연구자들의 이해를 돕고자 하였음

  ※ 각 사례는 실제 공개된 규정, 정책, 보도자료, 인터뷰, 내부 가이드라인 등을 바탕으로 정책적 이해를 돕기 위해 재구성·창작한 가상 사례이며, 특정 기관, 인물 또는 실제 사건과는 무관함

참고 국제공동연구 연구보안 길잡이 사용설명서

- 본 가이드라인의 주요 용어(영어 약자) 해설은 하단의 색인을 참조 바랍니다
- 본판은 미국 중심의 내용으로 구성되어 있으며, 향후 EU와의 협력 시 유의사항을 반영한 개정·증보판이 발간될 예정입니다.

제2장

국제공동연구와 연구보안

제2장. 국제공동연구와 연구보안

1 국제공동연구 근거와 정의 및 추진 유형

국제공동연구의 법적 근거

- 국제공동연구는 국내 연구기관과 해외 연구기관이 협력하여 연구개발(R&D)을 수행하는 형태로, 과학기술 발전과 국제 경쟁력 강화를 위해 필수적인 활동이며, 이를 뒷받침하는 주요 법적 근거는 다음과 같음

- **과학기술기본법**
  - 제18조에서는 과학기술의 국제화를 촉진하기 위해 정부가 국제협력을 강화하고, 연구개발 협력을 증진하도록 규정하여 국제공동연구를 활성화하기 위한 정책적 지원을 명문화

- **국가연구개발혁신법**
  - 국가연구개발사업의 전반적인 운영 및 관리 기준을 제시하며, 국제공동연구 추진 시 필요한 연구비 지원, 성과 관리, 보안 대책 등을 포함
  - 연구보안과 관련된 조항도 포함되어 있어, 연구성과 보호 및 연구보안 강화를 위한 법적 장치로 기능

- **국제사법 및 기타 법규**
  - 해외 연구기관과의 계약 및 협약 체결 시 준수해야 할 원칙을 규정
  - 계약상의 법적 분쟁 발생 시 적용할 법률과 해결 절차를 정의하여 국제공동연구의 안정적인 운영을 지원
  - 연구수행 과정에서는 『국제사법』, 『형법』, 『행정소송법』 등 다양한 법적 규정이 적용될 수 있음

- **국가연구개발사업 관련 시행령 및 고시**
  - 『국가연구개발사업 연구개발비 사용기준』(과학기술정보통신부고시)에서 연구비의 사용 및 관리 기준을 정함
  - 『국가연구개발사업 보안대책』(과학기술정보통신부고시)에서 연구보안의 기본 원칙과 관리 방안을 규정

국제공동연구의 개념과 범위

- 국제공동연구는 국내 기관(정부, 대학, 기업, 연구소 등)과 해외 기관이 협력하여 연구개발을 수행하는 활동을 의미하며, 다음과 같은 특징을 가짐
  - **(연구 주체)** 정부기관, 대학, 연구소, 기업 등 다양한 기관 간 협력이 가능하며, 연구주체 간 협력 방식에 따라 단순한 연구 교류부터 공동 연구개발 프로젝트까지 다양한 형태로 운영
  - **(연구 방식)** 논문 공동 작성 및 발표, 공동 연구시설 및 장비 활용, 기술 공동개발 및 연구성과 공유, 해외 연구자 초빙 및 파견 프로그램 운영
  - **(연구 범위)** 기술개발, 인프라 및 데이터 공유, 인력 양성, 정보 교류, 연구개발비, 연구개발 인력 및 시설 등 과학기술자원을 공동으로 투입하여 수행하는 연구 등을 포함하며, 연구 주제와 협력 수준에 따라 다르게 적용 가능

국제공동연구의 추진 유형

- 국제공동연구는 연구비 지원 방식, 연구 수행 방식, 연구성과의 공유 방식에 따라 다음과 같은 유형으로 구분

① 일반형

- 국내 연구개발기관이 해외 기관을 활용하여 연구를 수행하는 방식
- 연구비는 국내 연구기관이 관리하며, 해외 연구자는 연구 협력자로 참여
- 연구협약 및 계약 없이 논문 공동 집필, 공동 실험 등 협력이 이루어지는 경우도 포함

※ (예) 국내 대학이 해외 연구소와 협력하여 신소재 개발 연구를 수행

② 공동기관형

- 해외 기관이 공동 연구개발기관으로 참여하며, 연구비 일부를 직접 수령
- 연구책임자와 연구팀이 국경을 넘어 협력하며, 연구성과를 공동 소유
- 연구비 집행이 국내외에서 각각 이루어질 수 있으며, 공식 협약이 체결됨

※ (예) 한국과 유럽연합(EU)의 공동 연구 프로젝트에서 국내 연구소와 해외 대학이 공동으로 연구 수행

③ 별도과제형 (Joint Call)

- 연구내용은 연계되어 있지만, 연구비 집행 및 연구계획 수립은 각국의 기관에서 독립적으로 수행
- 연구비 지원 기관이 국가별로 다르며, 연구결과 공유 방식도 사전에 정의됨

※ (예) 한국과 미국의 공동 연구 프로그램에서 각각 독립적으로 연구 수행 후 연구성과 공유

국제공동연구의 기획 및 공고 절차

- 국제공동연구의 기획 및 공고 절차는 다음과 같은 단계로 진행
  - **(수요 조사)** 연구개발 필요성을 평가하고, 국제협력 대상 국가 및 연구기관을 선정, 정부 및 연구기관 차원에서 연구주제와 협력 가능성을 검토
  - **(사전 기획)** 연구과제의 목표 및 연구성과 활용 계획 수립, 연구개발비 조달 방식 및 연구성과 공유 방식 결정, 연구과제의 보안 등급 및 연구윤리 검토
  - **(공고 및 공모)** 연구개발계획서 작성 및 연구협력 기관과 협약 체결, 연구자 및 연구기관이 연구개발 과제 신청 및 참여, 국내외 연구기관이 공동 연구 수행을 위한 연구계획 수립
  - **(과제 선정 및 협약)** 연구계획서를 평가하여 최종 연구 협력 기관 선정, 연구 협약 체결 후 연구 수행 개시, 연구과제의 진행 상황을 지속적으로 모니터링하며, 연구성과를 관리
  - **(연구 수행 및 성과 공유)** 연구과제 수행 중 연구성과 보호 및 지식재산권 문제 해결, 연구성과 발표 및 국제적 활용 방안 마련
  - **(사후 평가 및 연구성과 확산)** 연구 성과의 산업적 활용 가능성 검토, 연구성과를 기반으로 후속 연구개발 계획 수립

국제공동연구의 성공적인 추진을 위한 고려사항

- **연구보안 :** 연구성과 보호 및 연구데이터 유출 방지를 위한 보안 대책 마련
- **지식재산권 관리 :** 연구성과의 공동 소유 및 특허 출원 시 명확한 협약 필요
- **연구비 집행 투명성 :** 국제공동연구에서 연구비 사용 내역을 명확히 관리해야 함
- **정책 및 규정 준수 :** 국가 간 연구협력 시 각국의 연구 관련 법률 및 규정 등 준수 필요

2 국제공동연구에서 연구보안의 중요성

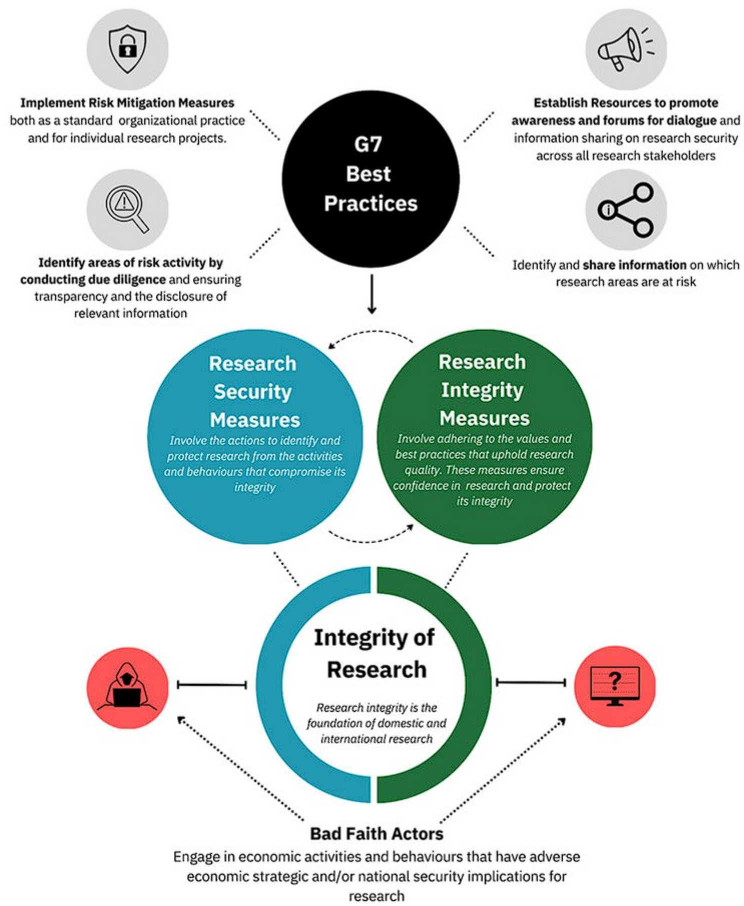
연구보안의 개념과 국제적 중요성

- 국제공동연구는 과학기술 발전을 가속화하고, 글로벌 도전과제 해결에 기여하는 핵심적인 연구 방식으로서, 기후 변화 대응, 감염병 연구, 우주 개발, 인공지능(AI) 등 다양한 분야의 난제 해결을 위한 필수적인 연구 형태로 부상 중
  - 이러한 개방성과 협력 중심의 연구 환경에서는 연구보안(research security)의 중요성이 점차 부각되고 있음
- 연구보안이란 연구활동 중 발생할 수 있는 경제적, 전략적, 국가 안보적 위험 요소로부터 연구 자산을 보호하는 것을 의미하며, 연구진실성(research integrity)과 함께 신뢰받는 연구 생태계를 유지하는 핵심 요소임
  - 연구보안은 연구자의 학문적 자유와 국제적 협력의 개방성을 유지하는 동시에, 지식재산권(IP) 보호, 데이터 보안, 연구 성과의 오남용 방지를 위해 필수적으로 고려되어야 함
  - 연구보안이 부재할 경우, 외국 기관이나 적대적 행위자에 의해 연구 성과가 무단으로 유출될 수 있으며, 이는 연구자의 정당한 공로를 훼손할 뿐만 아니라 국가 차원의 연구 경쟁력을 저하시킬 위험이 있음
- G7 국가들은 연구보안과 연구진실성이 상호 보완적인 개념이라는 점을 강조하고 있으며, 연구협력이 지속되기 위해서는 연구 성과의 보호와 개방성 간 균형이 필수적이라는 원칙을 천명하고 있음
  - 특히, 연구보안 조치는 불법적인 기술 이전, 지식재산권(IP) 침해, 연구 자산의 부적절한 활용 등을 방지하고, 연구자 및 연구기관이 신뢰할 수 있는 협력 환경을 조성하는 데 기여함
- 연구보안은 단순히 연구자 개인이나 특정 연구기관 차원의 문제가 아니라, 국가 차원의 정책 대응 및 국제적 협력이 요구되는 사안으로 볼 수 있음
  - 각국 정부는 체계적인 연구보안 정책을 수립·시행하고 있으며, 연구자 및 연구기관 또한 이에 대한 인식을 제고하고 보안 조치를 강화하기 위한 노력이 필요함
  - 아울러, 연구보안은 연구자 및 기관의 자율적 실천이 중요한 기반이 되나, 국제적 가이드라인 및 정부의 정책적 지원이 병행될 때 보다 효과적으로 구현될 수 있음

국제공동연구에서의 연구보안 주요 이슈

- 최근 미·중 간 기술패권 경쟁 등 글로벌 경쟁 구도가 심화됨에 따라, 과학기술은 단순한 학문적 탐구를 넘어 국가 경제 및 안보에 영향을 미치는 전략적 자산으로 인식되고 있음. 이에 따라 연구보안의 개념은 군사 및 경제 안보 영역까지 포괄하는 방향으로 확장되고 있으며, 주요국들은 관련 정책을 지속적으로 강화 중임
  - 미국, 일본, 영국, 호주 등은 연구보안 강화를 위해 외부자금 수혜 신고 의무화, 연구자 및 기관 대상 연구보안 가이드 배포, 연구보안 전담 조직 신설 등의 조치를 시행하고 있음
  - 미국 국립과학재단(NSF)은 연구안보정책실을 운영하고 있으며, 일본은 연구자의 이해상충을 방지하기 위해 연구 지원금 및 외국 자금 수혜 내역을 신고하도록 규정하고 있음
- 기술패권 경쟁 속에서 연구보안은 단순한 기술 보호 차원을 넘어 글로벌 협력 및 경제 안보와 밀접하게 연결되어 있음
  - 연구성과의 유출이나 악용은 자국의 핵심 산업 경쟁력을 악화시키고 국가 안보에 부정적 영향을 미칠 수 있으므로, 연구보안은 과학기술정책뿐 아니라 경제 안보 전략의 핵심 요소로 부상하고 있음
- 국제사회에서도 연구보안 관련 협력이 강화되고 있으며, G7은 연구보안 8대 원칙을 발표하며 연구보안의 필요성을 국제적으로 천명하고 있음

- G7 연구보안 원칙은 다음과 같은 내용을 포함
  - **(국익과 글로벌 이익의 균형 유지)** 국가별 연구보안 정책이 각국의 경제적·전략적 이익을 보호하면서도 국제 협력의 틀 안에서 조화를 이루어야 함을 강조
  - **(개방성과 연구보안의 조화)** 연구보안이 과도한 규제가 되어 개방성과 혁신을 저해하지 않도록 연구자 및 연구기관의 자율성을 존중해야 함
  - **(협력과 대화 촉진)** 연구보안은 일방적 조치가 아닌 국제적 대화를 통해 조율되어야 하며, 상호 신뢰를 바탕으로 연구 협력을 유지해야 함
  - **(사전 예방적 조치 강화)** 연구자 및 기관이 연구보안 위험을 사전에 인지하고 대응할 수 있도록 정보 공유 및 교육 필요
  - **(위험 수준에 따른 대응)** 연구 분야 및 연구 내용에 따라 차별화된 보안 조치를 적용하여 연구자들의 부담을 최소화하는 방안을 마련해야 함
  - **(공동 책임의 이행)** 연구보안은 연구자, 연구기관, 정부, 국제기구 등이 공동으로 책임을 지고 협력해야 하는 과제임
  - **(책임성과 투명성 강화)** 연구자 및 연구기관이 연구보안 관련 의무를 명확히 인식하고 준수할 수 있도록 투명한 기준을 마련해야 함
  - **(적응성과 유연성 확보)** 연구보안 정책은 기술 및 국제 환경의 변화에 따라 지속적으로 조정·개선되어야 함

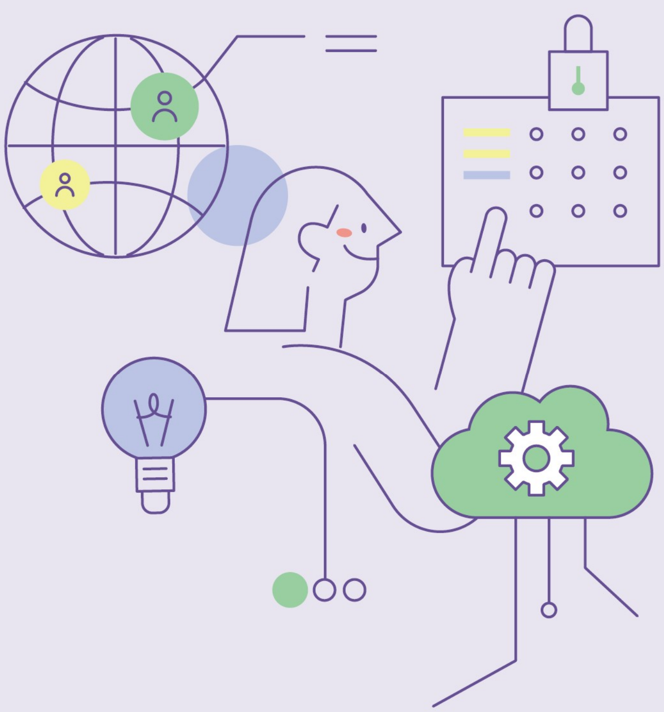


[그림 1] 연구보안과 연구진실성이 연구의 기초를 보호하는 방식

※ (출처) https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/international-research-security-resources/g7-common-values-and-principles-research-security-and-research-integrity

- 이러한 연구보안 원칙은 국제공동연구를 수행하는 과정에서 보안과 개방성 간 균형을 잡기 위해 정부뿐만 아니라 연구자 및 연구기관의 공동 노력이 필요함을 강조하고 있음

제3장



미국 연구보안 주요 제도·규정 및 유의사항

제3장. 미국 연구보안 주요 제도·규정 및 유의사항

1 개요

미국 정부는 자국 예산이 투입되는 연구 활동의 보안을 강화하기 위해 다양한 조치를 시행 중임

- 미국 정부 연구자금을 신청하거나 사용하는 우리나라 연구자들 또한 이러한 조치의 영향을 받을 수 있으므로, 각 자금 지원 기관이 요구하는 연구 보안 요건을 정확히 이해하고 준수할 필요가 있음
- 우리나라 연구자들은 미국과 국제공동연구를 수행할 때 다음 사항에 유의할 필요가 있음
  - 미국 각 자금 지원 기관이 설정한 연구보안 요건을 숙지
  - 미국 파트너와 협력하는 경우, 해당 기관의 요구사항에 대해 사전에 협의하는 것이 권장됨
  - 각 연구 자금 기회(RFO)에는 연구보안 요건을 충족하기 위해 따라야 할 구체적 절차와 요건이 명시되어 있으며, 이에 대한 정의와 요건은 미국 연구보안 관련 지침에 따름

미국 연구보안정책 관련 상위 법령·지침 및 주요 자금 지원 기관은 다음과 같음

- 주요 법령 및 지침
  - **2021년 국가안보대통령교서-33 (NSPM-33, National Security Presidential Memorandum-33)**
  - **2022년 과학기술정책국(OSTP)이 발표한 NSPM-33 연방기관 이행 지침**
  - **2022년 CHIPS 및 과학법**
- 미국 의회조사국(Congressional Research Service, CRS) 보고서에 따르면, **FY2025 연방 연구개발(R&D) 예산 요청**[1]에서 **주요 5개 기관의 예산 비율**을 합산 시 전체 연방 R&D 예산의 약 92.5%를 차지하며, 개별 기관별 규모는 다음과 같음
  - **국방부 (DoD) : 전체 R&D 예산의 41.8%**
  - **보건복지부(HHS) : 전체 R&D 예산의 27.1%**
  - **에너지부 (DOE) : 전체 R&D 예산의 11.6%**
  - **항공우주국 (NASA) : 전체 R&D 예산의 8.5%**
  - **국립과학재단 (NSF) : 전체 R&D 예산의 3.5%**

1) Sargent, J. F., & Gallo, M. E. (2024, March 27). Federal research and development (R&D) funding : FY2025 (CRS Report No. R48307). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R48307

참고 국가안보대통령교서-33 (NSPM-33(National Security Presidential Memorandum-33))

- 미국 바이든 행정부가 연방 자금을 받는 연구 활동의 보안과 무결성을 강화하는 것을 목적으로 2021년 1월 발표한 지침으로, 국제공동연구 및 외국의 부정한 영향으로부터 미국의 기초 및 응용과학의 경쟁력을 보호하려는 조치 중 하나
- NSPM-33은 △ 연구자 개인의 보고 의무 (Disclosure Requirements) △ 연구기관의 책임과 보안 체계 구축 (Research Security Programs) △SciENcv 시스템 통한 통합 보고 권장 등을 연구보안 관련 핵심 내용으로 규정
  - **연구자 개인의 보고 의무 (Disclosure Requirements)** : 연방 자금 수혜 대상자(PIs, Co-PIs, Senior Personnel 등)는 외국의 직책 및 소속, 외국 기관/정부의 연구지원 수혜 이력, 외국 정부와의 계약, 협약 이력, 외국 인재 유치 프로그램(FTRP) 참여 여부, 외국에서의 연구활동 및 공동연구 이력 등의 개인 정보를 의무적으로 제출하도록 요구
    - 특히 연구자는 악성 외국 인재 유치 프로그램(MFTRP, Malign Foreign Talent Recruitment Programs) 참여 여부를 서면으로 부인해야 하며, 참여 사실이 적발될 경우 지원 자격 제한 또는 제재
  - **연구기관의 책임과 보안 체계 구축 (Research Security Programs) :** 연구비를 수혜하는 기관 전체에 다음 요건을 요구
    - 정보보안 (Cybersecurity) : 연방 표준(NIST SP 800-171 등)에 따라 연구데이터 및 네트워크 보안 강화
    - 연구자 행동 관리 (Researcher Disclosure Policy) : 연구자의 외부 활동, 재정지원, 겸직 등 모든 이력의 포괄적·정기적 보고 체계 마련
    - 해외 협력 위험 평가 (Foreign Risk Management) : 공동연구 파트너의 국적, 기관 성격(군사적 목적 여부 등), 통제 기술 여부 등에 따른 사전 위험 분석
    - 연구보안 교육 및 인식 제고 : 연구자 대상 정기적 보안 교육 프로그램 운영 의무화

    ※ 이 네 가지 요소는 연방정부가 향후 모든 수혜기관이 갖추어야 할 인증 요건으로 제시하고 있으며, 연구보안 역량이 부족한 기관은 지원 자격이 제한될 수 있음
  - **SciENcv 시스템 통한 통합 보고 권장 :** SciENcv(Science Experts Network Curriculum Vitae)를 활용하여 연구자의 모든 경력·수혜 이력 보고를 통합 관리하고 있으며, NSF와 NIH 등 주요 기관은 이를 의무화 중
- 상기 연구보안 관련 규정 미준수 시 연구비 회수, 향후 연방과제 수주 제한, 법적 제재 가능
- NSPM-33은 연방 자금(federal funding)이 투입된 연구과제를 수행하는 연구자에게 적용되는 정책으로, 연방정부 자금을 직접적으로 포함하고 있는지 여부에 따라 적용 여부가 달라짐

참고 OSTP가 발표한 NSPM-33 연방기관 이행 지침

- 2022년 1월 OSTP(백악관 과학기술정책실)는 NSPM-33의 실제 이행을 위한 상세한 지침으로 "NSPM-33 Implementation Guidance" 문서를 발간하였으며, 이 지침은 연방 연구자금 수혜기관이 반드시 갖추어야 할 보안 체계와 연구자 보고 시스템의 표준화 기준을 제시
- 이 지침은 기관의 연구보안 프로그램 구성 요소를 4개 영역으로 구분하고, 보고 정보를 표준화하는 것을 목적으로 함
  - 기관의 연구보안 프로그램 구성 요소 (4대 영역) : OSTP는 연방 연구기관이 갖추어야 할 보안 요건을 아래 네 가지 분야로 명확히 규정
    - 정보보안 (Cybersecurity) : NIST SP 800-171 등 보안표준을 기반으로 시스템·데이터 보호체계 구축
    - 연구자 행동관리 (Researcher Disclosure Policies) : 외부 소속, 겸직, 재정지원 이력 등 의무적 보고 체계
    - 외국 영향 리스크 평가 (Foreign Risk Management) : 국가, 기관의 성격, 과제 위험도 분석을 기반으로 위험 평가
    - 교육 및 훈련 (Research Security Training) : 모든 연구자 대상의 주기적 보안 교육 이행 필수

    ※ 미 정부는 4대 요건이 일정 기준에 미달하는 기관은 연방 연구자금 지원을 받기 어렵도록 함
  - 보고 정보의 표준화(Disclosure Elements Checklist) : OSTP는 연구자 개인이 보고해야 할 사항을 소속 기관, 외국 정부 지원 모든 형태의 외국 자금 수혜 이력, 고용계약, 연구비 지원, 비금전적 지원, 외국 인재유치 프로그램 FTRP/MFTRP 참여 여부 등 13개 항목으로 표준화하였으며, 미국 연구기관은 이 Checklist를 기반으로 자체 보고양식 개발 또는 SciENcv 등 표준 플랫폼을 활용하여 보고 받도록 함

참고 CHIPS 및 과학법 내 연구보안 관련 조항

- 2022년 제정된 「CHIPS 및 과학법(CHIPS and Science Act)」은 연방 연구개발(R&D) 활동의 보안 강화를 위한 다양한 조항을 포함하고 있으며 이 법은 특히 외국의 부정한 영향으로부터 미국의 연구 생태계를 보호하고, 연구자 및 기관의 보안 의식을 제고하는 데 중점을 두고 있음
  - **연구보안 교육 의무화 :** 2025년 5월 1일부터, 연방 자금을 지원받는 연구 프로젝트에 참여하는 개인은 연구보안 교육을 이수해야 하며, 여기에는 연구책임자(PI), 공동연구자(Co-PI), 프로젝트 디렉터(PD), 박사후 연구원, 대학원생 등 주요 기여자가 포함되고, 교육 내용은 △사이버보안, △국제 협력 시 보안 고려사항, △외국의 부정한 영향 및 간섭 대응, △연구 무결성 및 위험 관리 등을 포함
  - **연구보안 프로그램 구축 요건 :** 연방 R&D 자금을 연간 5,000만 달러 이상 수령하는 기관은 사이버보안, 외국 여행 보안, 내부 위협 인식 및 식별, 수출 통제 교육 등의 요소를 포함하는 연구보안 프로그램을 구축해야 함
  - **악성 외국 인재 유치 프로그램(MFTRP) 참여 금지 :** 연방 연구 자금 수혜자는 악성 외국 인재 유치 프로그램(MFTRP)에 참여하지 않았음을 인증해야 하며, 참여 사실이 확인될 경우, 연구비 수혜 자격이 제한되거나 박탈 가능함
  - **외국 재정 지원 공개 의무 :** 연방 자금을 지원받는 고등교육기관은 외국의 우려 국가(foreign country of concern)로부터 받은 5만 달러 이상의 기부금 및 계약을 연간 보고해야 함
  - **국립과학재단(NSF) 내 연구보안 및 정책 사무소 설립 :** NSF는 △연구보안 정책 개발 및 모범 사례 수립, △연구 보안 관련 교육 및 홍보 활동 수행, △연구 제안서 및 수상에 대한 위험 평가 수행, △NSPM-33 준수를 위한 정책 수립 및 이행 등의 역할을 하는 '연구보안 및 정책 사무소를 유지

모든 R&D 자금 지원기관에 공통 적용되는 의무 사항 : MFTRP 및 FTRP 관련 보고 의무

※ 상세 보고 요건 등은 기관 내부 규정을 따르며, 기관에 따라 다소 차이가 있을 수 있음

- '대상 개인'(Designated Individual, 미국 연구 보안 정의 참조)은 다음 사항을 증명해야 함 :
  - 제안서 제출 시점 및 수상 기간 동안 매년, 본인이 악성 외국 인재 채용 프로그램(MFTRP)에 적극적으로 참여하고 있지 않음을 확인해야 함
  - 제안서 제출 시점 및 수상 기간 동안 매년, 모든 외국 인재 채용 프로그램(FTRP) 참여 여부를 완전하게 공개해야 함
- 시행 시점
  - NSF 과제의 경우 : 2024년 5월 20일부터 적용됨
  - 기타 모든 연방 및 비연방 외부 후원 과제 : 2024년 8월 9일부터 적용됨
- 과거 MFTRP 참여 이력에 대한 고려사항
  - 2022년 8월 9일 이전에 MFTRP에 참여한 이력이 있는 경우, 해당 사실이 포함된 제안서는 추가적인 검토 대상이 될 수 있음
  - 이 경우, 과제 수탁 기관의 판단에 따라 기관에 따라 완화조치(Mitigation Measures)가 요구될 수 있음

주요 연구보안 규정 요약

- ①정보 공개(Disclosure) 및 이해충돌 관리, ②외국 인재 유치 프로그램 제한, ③CUI(Controlled Unclassified Information) 및 수출통제, ④기술이전 통제, ⑤시스템 접근 및 시설 출입 통제, ⑥출국 및 출장 통제 등의 연구보안 규정을 운영 중

| 표 1 | 주요 연구보안 규정 요약

구분	주요 내용
정보 공개 (Disclosure) 및 이해충돌 관리	• 외국 소속, 자금, 인재 프로그램 참여 이력 등에 대한 의무적 공개 요구
외국 인재 유치 프로그램 제한	• MFTRP 참여 금지 및 증명 의무 • MFTRP 참여자는 미국 연방과제 참여 제한 또는 자금 지원 불가
CUI 및 수출통제(Export Control)	• 민감 기술에 대한 외국인 접근 제한 및 시스템 통제 • 외국 연구자의 접근은 사전 승인, 보안 교육 이수, 최소 권한 원칙에 기반하여 관리
기술이전 통제	• 외국 협력 시 기술 범위·제공자료·보안 수단 등을 명확히 설정해야 함
시스템 접근 및 시설 출입 통제	• 시스템 계정, 연구시설 방문, 소프트웨어 접근 등과 관련하여 사전 보안 승인 절차가 필수적으로 요구됨
출국 및 출장 통제	• 연구 목적으로 미국 내 국방 또는 에너지 관련 시설을 방문할 경우, 추가적인 심사 절차가 요구됨

참고 미국 연구보안 주요 공통 정의 및 요구사항

- 미국 연구보안 정책 관련 상위 법령·지침인 국가안보대통령교서-33 (NSPM-33), NSPM-33 연방기관 이행 지침, 2022년 CHIPS 및 과학법 등에서 공통적으로 사용하는 연구보안 관련 용어 및 요구사항 등은 다음과 같음
- 소속(Affiliation)
  - 학부생 및 대학원생을 제외한 학술적·전문적·기관적 임명 또는 직위로, 외국 정부 또는 외국 정부 연계 기관과의 관계를 포함
  - 전일제, 시간제, 자원봉사(겸임, 방문, 박사후 과정, 명예직 포함) 여부와 상관없이 금전적·비금전적 보상 또는 그에 상응하는 대가성 의무가 수반되는 경우를 포함
- 연계(Association)
  - 학부생 및 대학원생을 제외한 학술적·전문적·기관적 임명 또는 직위로, 외국 정부 또는 외국 정부 연계 기관과의 관계를 포함하나, 금전적·비금전적 보상이나 대가성 의무가 없는 경우를 의미함
- 해당 인물(Covered Individual 또는 Senior/Key Personnel)
  - 법률 제10638조에 따르면, '해당 인물'은 다음 요건을 모두 충족하는 자를 의미
    - 연방 연구기관으로부터 연구개발 자금을 지원받아 수행되는 과제에 대해 과학적 개발 또는 수행에 실질적이고 의미 있는 기여를 하는 자
    - 해당 연방 연구기관이 '해당 인물'로 별도로 지정한 자 (기관별로 사명에 따라 추가 지정 가능)
  - NSPM-33에 따르면, 일반적으로 연구책임자(PI), 주요 연구자, 그리고 연방 연구기관 실험실/시설 소속 연구자 (내부 연구자)를 포함하며, 여기에는 정부 소유·민간 운영(GOCO) 실험실 및 시설 소속 인력도 포함됨
- 우려 국가(Foreign Countries of Concern, FCOC)
  - 미국 정부가 연방법(10 U.S.C. 4872(d))에 따라 지정한 우려 국가에는 중국, 북한, 러시아, 이란이 포함됨
- 선물(Gift)
  - 대가 없이 제공되는 것을 의미하며, 모든 사례금, 호의, 할인, 오락, 환대, 대출, 관용, 라이선스, 특별 접근, 장비 시간, 샘플, 연구 데이터 또는 금전적 가치가 있는 기타 항목 포함
  - 현물, 티켓 구매, 선불 또는 비용이 발생한 후 상환 여부에 관계없이 교육, 교통, 지역 여행, 숙박, 식사, 연구 시간 등의 서비스와 선물도 포함
- 외국 인재 채용 프로그램 (Foreign Talent Recruitment Program, FTRP)
  - 외국 정부 또는 연계 기관 주관의 프로그램, 직위 또는 활동으로서 아래 형태의 보상이 포함되는 경우 해당됨. 해당 보상은 국가 차원(중앙/지방) 또는 대리 기관을 통해 직접 또는 간접적으로 제공될 수 있고, 보상이 서면 계약·문서 등에 명시되지 않더라도 아래 조건을 만족한다면 포함
    - 현금 보상, 현물 보상 (연구비 포함), 향후 보상 약속, 무료 해외여행, 비경미성(non de minimis) 물품, 명예직 또는 직위, 경력 발전 기회 등
  - **FTRP에 해당하지 않는 국제협력 활동**은 다음과 같음 (단, 2019년 국방수권법에 따른 특정 리스트에 포함된 제재기관 주관일 경우 제외) :

- 과학 정보의 학술 발표 및 출판 (법령에 의해 통제되지 않는 경우)
- 상호 개방적이고 투명한 정보 교류가 있는 국제 회의, 교류, 프로젝트 참여
- 외국 유학생에 대한 조언 및 추천서 제공
- 다음과 같은 국제 활동 참여 :
  1. 미국 정부 일부가 후원한 이사회 활동(예 : 미-이스라엘 공동과학기금)
  2. 국제기술기구, 표준화기구, 다자과학기구 활동
  3. 풀브라이트 등 공공재정 국제교류 프로그램
  4. 국제 학회, 학술원(예 : 로열 소사이어티 등) 활동
  5. 방문학자, 안식년, 박사 또는 전문자격 취득 관련 학술 활동
  6. 연구개발 업적에 따른 국제상 수상 (예 : 노벨상)

- 악성 외국 인재 채용 프로그램 (Malign Foreign Talent Recruitment Program, MFTRP)
  - 다음과 같은 조건에 해당할 경우, **악성 외국 인재 채용 프로그램(MFTRP)으로 간주**
    - 외국 정부 또는 그 연계 기관으로부터 현금·현물·명예직·경력 기회 등을 수령하고
    - 이에 더해 다음 중 하나 이상을 요구받는 경우 :
      1. 지식재산, 데이터, 비공개 정보를 무단으로 외국 정부 또는 기관에 이전
      2. 타 연구자 또는 학생의 MFTRP 참여 모집
      3. 외국에서의 실험실 설립, 교수직 수락, 회사 설립 등 수행 (연방 R&D 계약 위반 시 해당)
      4. 특별한 사유 없이 계약 해지가 불가능한 조건
      5. 해당 활동으로 인한 미국 연구 활동 수행 능력 제한 또는 중복 수행 유도
      6. 외국 정부 자금 신청 의무
      7. 본인 소속기관 또는 연방연구기관의 명시를 고의로 생략하도록 요구
      8. 본 프로그램 참여 사실을 본인 고용기관 또는 연구기관에 보고하지 않도록 요구
      9. 보조금 이해 상충 또는 책임 상충을 유발
  - MFTRP로 간주되는 추가 조건은 다음과 같음
    - 우려국가 또는 그 연계 기관에서 운영 또는 후원
    - 국방수권법 제1286조(c)(8), (9)상 '문제 기관' 으로 분류
    - 외국 인재 프로그램 명단에 포함된 프로그램
  - **MFTRP로 간주되지 않는 활동**은 다음과 같음
    - 과학 정보 발표 및 출판 (법률 통제 대상 제외)
    - 국제 회의·연구 프로젝트 등 상호 정보 교류 기반 협력
    - 외국 유학생에 대한 지도 및 추천서 제공 요청 응답

2 에너지부(DOE)

개요

미국 에너지부(DOE)는 국제협력과 개방형 혁신을 지향함과 동시에, 연구보안을 강화하기 위한 체계적인 정책을 수립·운영 중임

- DOE는 국제공동연구 추진 시 외국 기관 및 연구자와의 협력이 미국의 국가이익, 안보 전략, 산업경쟁력, 정보보호 등 관련 기준에 부합하는 경우에 한해 국제공동연구를 수행
- 단순한 기술 통제나 계약 심사를 넘어서, 개인·기술·제도 전반에 걸친 선제적 통제 체계를 운영
- 연구자의 이력, 기술의 민감도, 기관 협력의 전략 정합성, 산업적 기여도 등을 종합적으로 평가하여 협력 여부를 승인

참고 DOE의 주요 연구보안 규정

- **외국 정부 후원 또는 제휴 활동** : DOE Order 486.1A, Foreign Government Sponsored or Affiliated Activities
- **DOE 국립 연구소와의 해외 교류** : DOE Policy 485.1A, Foreign Engagements with DOE National Laboratories
- **협동연구개발계약** : DOE Order 483.1B Change 2, Cooperative Research and Development Agreements (CRADA)
- **전략적 파트너십 프로그램** : DOE Order 481.1E Change 1, Strategic Partnership Projects (SPPs)
- **비밀이 아닌 외국인 접근 프로그램** : DOE Order 142.3B, Unclassified Foreign National Access Program
- **공식 외국 출장** : DOE Order 550.1 Change 1 (LtdChg), Official Travel
- **과학기술 위험 매트릭스** : Science & Technology Risk Matrix

DOE의 국제공동연구 관련 연구보안 접근

DOE의 국제공동연구 관련 연구보안 접근의 특성은 ①개인 기반 관리, ②사업·기술 기반 관리의 두 가지 차원으로 이해 가능

① (개인 기반 관리) 개인 신원 및 외국 연계 활동의 선제적 식별·통제

※ (관련 규정) **DOE O 486.1A**(외국 정부 후원 또는 제휴 활동), **DOE O 142.3B**(비밀이 아닌 외국인 접근 프로그램), **DOE O 550.1 Chg 1** (공식 외국 출장)

- DOE는 연구자의 국적, 경력, 외국 정부와의 관계, 외국 자금 수령 또는 직위 수락 여부 등을 면밀히 검토함
- 특히 외국 정부 인재 유치 프로그램(FTRP) 참여 이력이나 외국 기관과의 관계는 협력 제한 또는 사전 보고·승인 대상이 됨

② (사업·기술 기반 관리) 국제공동연구는 미국의 국익 및 DOE 정책 목표와의 정합성 및 기술 민감도 등을 기반으로 승인되며, 기술의 민감도는 S&T Risk Matrix에 따라 등급화

※ (관련 규정) **DOE P 485.1A**(DOE 국립연구소와의 해외 교류), **DOE O 481.1E Chg 1**(전략적 파트너십 프로그램), **DOE O 483.1B Chg 2**(협동연구개발계약(CRADA)), **S&T Risk Matrix**(과학기술 위험 분류 기준)

- 국립연구소와의 MOU, CRADA, SPP 등은 기술적 필요성 외에도 미국 산업·외교·안보 전략과의 일치 여부가 검토되며, DOE 본부(HQ)의 보안·법무·외교 담당 부서의 사전 심사를 통해 승인
- 신흥 기술(emerging technology)에 대해서는 DOE의 S&T Risk Matrix를 활용하여 Red, Yellow, Green 등급으로 사전 분류하며, 민감 기술에 대해서는 외국인 접근 제한 및 면제 절차 적용 요구

| 표 2 | DOE 연구보안 접근 차원별 관련 규정

구분	주요 내용	관련 규정
① 개인 기반 관리	외국 정부와의 연계, 인재 프로그램(FTRP) 참여, 외국 자금 수령, 외국 직위 수락 여부 등을 사전 식별 및 통제	• DOE O 486.1A (Foreign Government Sponsored or Affiliated Activities) • DOE O 142.3B (Unclassified Foreign National Access Program) • DOE O 550.1 Chg 1 (Official Foreign Travel)
② 사업·기술 기반 관리	신흥 기술을 S&T Risk Matrix에 따라 Red, Yellow, Green으로 분류하고, 등급에 따라 외국인 접근 제한 및 면제 절차 운영, CRADA, SPP, MOU 등 국제공동연구는 미국 국익, DOE 정책 목표, 기술안보, 외교 전략과의 정합성 기반으로 승인	• S&T Risk Matrix ('22.12.17.) • DOE P 485.1A (Foreign Engagements) • DOE O 483.1B (CRADA) • DOE O 481.1E (SPP)

본고는 이러한 DOE 연구보안의 접근 세 가지 특성 및 관련 규정들을 중심으로 우리나라 연구자 및 기관이 DOE와 국제공동연구 추진 시 유의해야 할 사항을 안내하고자 함

※ 본 7개 연구보안 규정은 DOE 및 산하 국립연구소 전체를 아우르는 총괄 사항으로, 실제 국제공동연구시 적용되는 연구보안 규정 및 관리 수준은 각 연구소별로 다소 차이가 있을 수 있음을 유의

참고 DOE 연구보안 규정이 적용되는 협력 유형

- 국제공동연구 유형 중 일반형*, 공동기관형**은 상당수 CRADA 체결을 요구하나, 별도과제형(Joint Call)***의 경우 CRADA 체결을 요구하지 않는 경우가 많음. **후술할 연구보안 규정은 CRADA 등을 공식 체결한 경우 적용될 수 있는 사항임에 유의**

* **(일반형)** 국내 연구개발기관이 해외 기관을 활용하여 연구를 수행하는 방식. 연구비는 국내 연구기관이 관리하며, 해외 연구자는 연구 협력자로 참여. 연구협약 및 계약 없이 논문 공동 집필, 공동 실험 등 협력이 이루어지는 경우도 포함 (예 : 국내 대학이 해외 연구소와 협력하여 신소재 개발 연구를 수행)

** **(공동기관형)** 해외 기관이 공동 연구개발기관으로 참여하며, 연구비 일부를 직접 수령. 연구책임자와 연구팀이 국경을 넘어 협력하며, 연구성과를 공동 소유. 연구비 집행이 국내외에서 각각 이루어질 수 있으며, 공식 협약이 체결됨 (예 : 한국과 유럽연합(EU)의 공동 연구 프로젝트에서 국내 연구소와 해외 대학이 공동으로 연구 수행)

*** **(별도과제형)** 연구내용은 연계되어 있지만, 연구비 집행 및 연구계획 수립은 각국의 기관에서 독립적으로 수행. 연구비 지원 기관이 국가별로 다르며, 연구결과 공유 방식도 사전에 정의됨 (예 : 한국과 미국의 공동 연구 프로그램에서 각각 독립적으로 연구 수행 후 연구성과 공유)

참고 DOE의 기타 연구보안 관련 규정 및 법령

※ DOE 연구보안 페이지에 직접 명시되지는 않았으나, 연구보안 관련성이 있는 규정 및 법령

- **에너지부 사이버보안 프로그램** : DOE O 205.1D, Department of Energy Cybersecurity Program
  - (휴대용 전자기기 보안) 해외 이동(foreign travel) 관련, 승인된 이동 범위 내 민감국가를 방문하는 직원에 대한 출국 전 브리핑 및 위험 평가를 수행하며, 해당 브리핑은 정부지급장비 보관 및 연결에 대한 지침과 분실 장치보고 절차를 제공
- **개인 보안** : DOE O 472.2A, Personnel Security
  - (비공식 해외이동 보고) 보안 허가를 신청하는 모든 신청자와 보안 허가/접근 권한을 보유하거나 국가 안보 관련 직책을 맡고 있는 개인은 비공식(개인적) 해외이동 전 계획을 해당 인적보안국에 보고해야하며, 특히 민감국가로 가는 경우, 이동 전 로컬 방첩조직으로부터 적절한 방어적 방첩 브리핑을 받아야 하며, 민감국가 이동일정 변경(deviation) 시 귀국 즉시(근무일 5일 이내) 보고해야함
  - (기타 보고 정보) 직계 가족이 민감국가에 거주하는 경우, 사건발생(occurrence) 후 근무일 3일 이내에 해당 인적보안국에 서면 보고
- **방첩 프로그램** : DOE O 475.1, Counterintelligence Program
  - (방첩(CI) 프로그램 평가) CI 프로그램 개선을 위한 성과평가 대상 중 하나로, 민감국가 인력들과 전문적, 개인적, 지속적인, 또는 재정적 접촉이 있는 개인들의 CI 브리핑과 보고를 통해 수집, 평가, 기록, 보고된 데이터의 품질 평가
  - (신원 확인) 테러리스트 또는 민감국가 인력, 민감주제, 보안구역 방문 관련 미분류(unclassified) 외국인 방문·임무 배치는 접근일 30일 전에 신원 확인을 요청해야 함
  - (이해관계자 책무) △민감국가 인력과 민감주제에 대해 논의 예정 또는 논의한 적이 있는 국가로 공식 방문하는 DOE 직원에 대한 CI 브리핑/보고(회의, 우연한 만남 등 포함), △민감국가 소속(affiliated) 인력과의 전문적/개인적/지속적/재정적 관계 보고, △민감국가 인력과 전문적 접촉 및 관계(발생지 무관) 보고, △외국 재정이 지원되는 모든 해외이동(민감국가, 비민감국가 포함) 보고 등을 위한 방첩국(OCI) 국장, DOE/ NNSA 현장·연구소·시설관리자, DOE 연방직원 등의 의무 명시
- **50 U.S. Code § 2652** – Restrictions on access to national security laboratories by foreign visitors from sensitive countries

  ※ 미국 연방 법률
  - DOE 장관/핵안보 청장은 민감국가의 시민/대리인에 대해 배경조사를 먼저 완료하지 않는 한, 국가안보연구소*, 핵무기생산시설**, 미 해군함정 핵추진 관련 기술·물질의 보호·개발·유지·처분을 직접 지원하는 부지로의 접근을 제한

    * (국가안보연구소) LANL, SNL, LLNL

    ** (핵무기생산시설) The Kansas City National Security Campus, The Pantex Plant, The Y-12 National Security Complex, The Savannah River Site, The Nevada National Security Site
    - 특히, 지정국가(covered foreign nation)*인 중국, 러시아, 북한, 이란에 대해서는 시설 접근 전 30일 이전에 의회에 국가 안보 이익 부합, 기밀·제한 데이터 미공개 등을 증명하는 면제 상황을 제외하고는 출입 제한하는 것으로 규제 강화('25.4.15 발효)

      * 50 USC § 3059(e)(1)에 근거

1 개인 기반 관리

관련 DOE 규정

- **외국 정부 후원 또는 제휴 활동** : DOE O 486.1A (Foreign Government Sponsored or Affiliated Activities) ('20.9.4.)
- **비밀이 아닌 외국인 접근 프로그램** : DOE O 142.3B (Unclassified Foreign National Access Program) ('21.1.15.)
- **공식 외국 출장** : DOE O 550.1 Chg 1 : Official Travel ('19.5.2.)

1) 위험국가 관련 외국 정부 연계 활동에 대한 통제

※ (관련 규정) **DOE O 486.1A**

- **(FGTRP 금지)** DOE 직원(Employee) 및 Contractor Personnel*의 **위험국가(Countries of Risk)와 관련된 인재 유치 프로그램(FGTRP : Foreign Government-Sponsored Talent Recruitment Program)에 대한 참여를 원칙적으로 금지**함

  * **(Contractor Personnel)** CRADA를 통해 공동연구를 수행하는 우리나라 연구자도 포함됨

  ※ 위험국가 목록은 DOE 홈페이지 (https://www.energy.gov/science/countries-risk)에 명시되어 있으며, 변동 가능. '25년 5월 기준 위험국가 목록은 중국·러시아·이란·북한·벨라루스임

- **(기타 외국 정부 연계 활동 제한)** DOE 직원(Employee) 및 Contractor Employee*는 위험국가 관련 **기타 외국 정부 연계 활동**(Other Foreign Government Sponsored or Affiliated Activities)의 경우, DOE 장관 또는 고위 승인권자의 **사전 서면 승인 하에서만 참여 가능**

  * **(Contractor Employee)** DOE와 고용 관계가 있는 특수한 경우를 의미하며, 일반적으로 국내 기관에 소속되어 CRADA 등을 통해 공동연구를 수행하는 연구자는 포함되지 않음

  - 외국정부 자금 수령, 외국기관의 연구 프로젝트 자문, 겸직, 외국정부 주도 프로그램 참여 등이 해당
  - 외형상 민간 활동이라 해도 자금 출처, 결정 구조, 조직 소속성 등을 통해 외국 정부 연계성이 확인되면 본 조항 적용 대상이 됨

- 이러한 활동은 DOE 본부 윤리책임자(DAEO) 또는 계약책임자가 판단하여 **승인 또는 중단 여부를 결정**하며, **사전 보고 누락 또는 허위 신고** 시, **협력 중단 및 향후 연구참여 제한 등의 제재가 부과**될 수 있음

참고 본 규정의 적용 대상 및 유의사항

- **(적용 대상)** DOE O 486.1A, 제1절(Purpose)에 따르면 적용 대상은 다음과 같음
  - **(FGTRP 금지)** DOE 직원 및 Contractor Personnel은 FGTRP 금지 대상인데, 이 중 **Contractor Personnel은 CRADA를 통해 공동연구를 수행하는 연구자도 포함 가능**
    - (Contractor Personnel) DOE O 486.1A, Attachment 2, 4.c.에 따르면, "CRADA, SPP, ACT 범위 내에서 DOE/NNSA 사이트 또는 임대공간에서 보수 수령 여부와 무관하게 R&D를 수행하는 개인"인 연구자는 "Contractor Personnel"로 간주되어 본 규정의 적용 대상임
    - (Contractor Personnel 예외 조항) DOE O 486.1A, 3. c. 및 Attachment 2의 4. Contractor Personnel 조항 중 예외 조항(d항)에 따르면 ①DOE 프로그램이 주도하는 국제협력 프로젝트를 구체적으로 이행하는 활동을 수행하면서 동시에 ② DOE 차원 또는 미국 정부 차원의 양자 또는 다자간 국제협정의 범위 내에 있는 활동을 수행하는 연구자는 본 규정의 면제 대상임

      ※ 따라서 우리나라 연구자가 본 규정의 적용 대상인지는 개별 프로젝트의 성격에 따라 상이할 수 있으므로, 적용 여부가 불확실하다면 소속 연구기관 내 계약 담당자 등에게 문의하거나 DOE 산하 국립연구소 등 협력 상대 기관 측에 문의 권장
  - **(기타 외국 정부 연계 활동 제한)** DOE 직원 및 Contractor Employee로 **일반적으로 DOE와 고용 관계가 있는 직원에 한정되며, CRADA를 통해 공동연구를 수행하는 국내 기관 소속 연구자는 제외됨**
    - (Contractor Employee) DOE와 CRD(Contractor Requirements Documents)가 포함된 계약 하에서 고용된 계약자 직원으로, 일반적으로 DOE와 고용 계약을 맺은 직원을 의미
- **(유의사항)** 일반적으로 CRADA 체결은 **DOE O 483.1B(CRADA)** 규정에 따라 진행되는데 해당 규정에 **FGTRP 관련 직접 언급은 없으므로**, DOE나 산하 국립연구소로부터 **FGTRP 관련 정보를 요청받는 경우는 많지 않음**
  - CRADA 체결 시 DOE O 483.1B 규정에 따라 **외국 소유·지배·영향 여부(FOCI) 심사**를 실시함
  - 그러나, **DOE O 486.1A** 규정에 따라 국제공동연구를 수행하는 연구자(Contractor Personnel)에게도 **FGTRP관련 정보를 요구할 수 있는 근거 조항이 존재한다는 점에 유의 필요**
  - 따라서 CRADA 체결 시 **DOE 또는 산하 국립연구소 측에서 FGTRP 관련 정보를 요청할 경우 해당 정보를 투명하게 공개**할 필요

2) 외국인 신원 조사 및 DOE 자산 등 접근 통제

※ (관련 규정) **DOE O 142.3B**

- 미국 외 국적을 가진 **외국인의 DOE 시설, 정보, 기술에 대한 접근을 통제**하기 위한 기준 명시
- 한국을 포함한 모든 **비 미국 국적자(Foreign National)**는 DOE와의 협력 또는 방문 시 다음 서류 제출 및 해당 절차를 이행해야 함

| 표 3 | DOE O 142.3B에 따른 주요 요구 사항

항목	내용
Access Request	• 외국인에 대한 사전 승인 필수. FACTS 시스템에 등록 필요
이력서(CV)	• 18세 이후 모든 경력·학력 포함. 10년 간 공백 없어야 함
민감 주제(Sensitive Subjects)	• 지정된 민감 기술 분야는 추가 심사 대상
이민/비자 상태	• 합법적인 체류 신분이 있어야 하며, 기간은 협력 기간과 일치해야 함
국가 위험도 평가	• “Countries of Risk” (위험 국가) 소속자는 제한 기술 접근 금지 또는 면제 필요
테러지원국 출신자(SST)	• SST 국적자는 특별 승인 필요 (DOE 장관급 결정)
신원 조사(Indices Check)	• 일부 협력 유형은 사전 CI(정보기관) 검토 필수
동반자 및 호스트	• 반드시 DOE 직원 또는 승인된 계약자가 호스트로 지정되어야 하며, 일정 요건 충족 필요

- **위험국가** 국적자 또는 기관이 **Red 등급 기술**에 접근할 경우 DOE 본부 및 현장 차원의 심사 및 승인 강화

※ **(면제 요청 절차)** ①DOE 현장 책임자가 승인 의향 여부 확인 → ②면제 사유 및 미국 국익 관련성 서술 → ③ PSO, CSO, FOAB 검토 후 Under Secretary 최종 승인 → ④정보기관(IN)의 강화된 배경 심사 필수 (최소 45일 소요)

참고 본 규정의 적용 대상 및 면제 요건

• **(적용 대상)** DOE O 142.3B, 제3절(Applicability) 및 Attachment 1 – CRD에 따른 적용 대상은 다음과 같음

- **(DOE 본부 및 소속 부서)** DOE 본부, 각 본부 부서, 현장 부서, CSOs(Cognizant Secritarial Officers), PSOs(Program Secretarial Officers), Under Secretaries incuding Science/Energy/Nuclear Security
- **(NNSA)** NNSA 소속 부서 및 직원
- **(DOE/NNSA 계약자)** DOE/NNSA가 소유·임대한 장소(site), 정보 또는 기술에 대한 외국인의 접근을 계약에 포함하는 계약자
  - DOE O 142.3B Attachment 1 – CRD, Section 4.a에 따르면 Hosting Site는 계약자가 운영하는 국립연구소를 포함할 수 있다고(may include) 명시
- **(하도급자)** 모든 계약자의 하도급자(Subcontractor)
- **(외국인)** DOE/NNSA 장소, 정보, 기술에 접근하려는 모든 외국인
  - **협력 유형과 무관**하게 DOE/NNSA 장소, 정보, 기술에 접근하려는 **모든 외국인에 적용된다는 점을 유의**

• **(면제 요건)** DOE O 142.3B, 제3절(Applicability) c항(Equivalencies/Exemptions for DOE O 142.3B)에 의거, 다음의 경우에는 본 규정의 면제 대상으로 별도 승인 없이 접근 가능

- 미국 이외 지역에서의 활동, 미국 국적 병행 보유자 (dual citizen with U.S.), 공개된 정보만 접근하는 경우, DOE가 참여하는 공식 국제협력 프로젝트 참여자, 공개 행사, 일반접근구역(General Access Areas, GAA) 내에서의 비업무 목적 방문 (개인 친지 방문 등) 등 특정 활동, 비상시 접근이 필요한 외국의 비상 대응인력 및 의료 인력, 미성년자 외국인(만 17세 이하), IAEA 공식 사찰단

※ DOE 산하 국립연구소와 공동연구 시 본 규정의 적용 대상 및 면제 요건 등 보안관리 수준은 개별 국립연구소마다 다를 수 있음을 유의

3) DOE 직원의 우리나라 출장 시 유의사항

※ (관련 규정) **DOE O 550.1 Chg 1** : Official Travel ('19.5.2.)

※ (참고) DOE 출장 규정은 **우리나라가 아닌 DOE 관계자가 준수하는 사항**이며, 특히 **DOE 산하 국립연구소별로 출장 규정 및 관리 수준 등이 상이**할 수 있으므로, **우리나라 측에서 DOE 및 국립연구소 관계자에게 선제적으로 안내 또는 요청을 할 필요는 없음을 유의**

- DOE 소속 직원이 대한민국을 포함한 모든 해외 국가로 출장하거나 외국 기관과 협력 활동을 수행할 경우, 반드시 DOE 공식 출장 승인 체계인 FTMS(Foreign Travel Management System)에 등록하고 사전 승인을 받아야 함
- 출장 내용에 민감국가(Sensitive Country) 방문 또는 민감 주제(Sensitive Subject)와 관련된 활동(예 : 발표, 협의 등)이 포함될 경우 :
  - DOE 정보국(Office of Intelligence and Counterintelligence, IN)의 사전 방첩 브리핑을 필수로 요구하며, 사후 보고 절차 역시 요구될 수 있음
  - 사용 예정 자료(발표 슬라이드, 논문 초안 등)가 있는 경우, 파견 전 보안 검토 또는 분류 여부 심사가 필요할 수 있음
  - 출장 목적, 방문 기관, 접촉 대상자, 협력 주제 등은 FTMS에 명확하고 구체적으로 등록해야 하며, 변경 시 갱신 필요

참고 본 규정의 적용 대상 및 면제 요건

- **(적용 대상)** DOE O 550.1, 제3절(Applicability) a항 및 b항에 따른 적용 대상은 다음과 같음
  - DOE 부서 전체(All DOE elements)
  - NNSA
  - DOE 계약자 (DOE와 체결한 site/facility management contract에 Attachment 1에 명시된 Contractor Requirements Document가 포함된 경우*)

  * 우리나라 기관이 DOE와 체결한 CRADA는 일반적으로 site/facility management 계약에 해당하지 않으며, 해당 계약에 CRD가 명시적으로 포함되어 있지 않은 한 당해 기관 및 소속 연구자는 DOE O 550.1의 직접적인 적용 대상인 "DOE 계약자"에 해당하지 않음. 다만, DOE가 개별 협약(CRADA) 체결 시 별도의 계약 조건을 통해 본 지침상의 일부 요건(예: FTMS 등록, 여권 요건, 사전 승인 절차 등)을 협력기관 또는 연구자에게 요구하는 경우, 해당 계약상 의무로서 이행이 요구될 수 있으므로 개별 CRADA 계약서의 관련 조항을 검토하는 것이 필요

- **(면제 요건)** DOE O 550.1, 제3절(Applicability) c항에 의거, 다음의 경우에는 본 규정의 면제 대상임
  - 보조금 수혜자(Grantees)
  - 연방에너지규제위원회(FERC, Federal Energy Regulatory Commission)
  - 해군 원자로 프로그램(Naval Reactors)

  ※ DOE O 550.1에 명시된 출장 규정은 DOE 및 산하 국립연구소 직원들이 준수해야 하는 규정임

  ※ DOE 산하 국립연구소와 공동연구 시 본 규정의 적용 대상 및 면제 요건 등 보안관리 수준은 개별 국립연구소마다 다를 수 있음을 유의

Tip! DOE와 CRADA를 통해 협력하고자 하는 연구자를 위한 상세 유의사항

〈 개인 신원 및 외국 연계 활동의 선제적 식별·통제 관련 유의사항 〉

1. CRADA 체결 시 DOE 또는 산하 국립연구소 측에서 FGTRP 관련 정보를 요청할 가능성이 존재함을 인지

- CRADA 규정에 FGTRP에 대한 직접 언급은 없으므로 실제 CRADA 체결 시 FGTRP 이력을 요청하는 절차가 있는 경우는 드물지만, DOE O 486.1A 규정에 의거하여 FGTRP 이력을 요구할 가능성이 존재함을 인식

☑ Tip | DOE 또는 산하 국립연구소 측에서 FGTRP 참여 이력을 요청할 경우, 연구자들의 관련 이력을 사전에 준비하는 것을 권장

2. CRADA 등 협력 여부와 무관하게 DOE 시설 또는 정보 접근 시에는 반드시 "호스트(Host)" 지정 필요

※ (참고) DOE 사업 참여뿐만 아니라 일반적 협력 시에도 DOE 시설 또는 정보 접근 시 호스트 지정 필요

- 우리나라 연구자가 DOE 연구소 또는 회의에 참석하려면, DOE 소속의 직원 또는 승인된 계약자가 반드시 호스트로 지정되어야 함
- 호스트는 ①방문 목적 및 신원 확인, ②사전 위험도 평가 요청, ③현장 동행 및 정보 접근 통제를 책임

☑ Tip | 협력할 DOE 파트너(연구자 등)가 방문 신청을 도와줄 수 있도록 사전에 협의하고 호스트 지정 요청

3. 이력서(CV) 및 개인 정보 제출 요건 유의

- DOE 방문 신청 시, 요청받은 사항에 부합하는 이력서 제출 필요

※ 개별 국립연구소에 따라 정보 제출 범위가 다를 수 있으므로, 안내받은 사항에 따라 관련 정보 제출 필요

☑ Tip | CV는 DOE 포맷 요구사항에 맞춰 사전 작성하고, 비자 정보도 포함하여 최신 상태로 유지를 권장

4. Red 기술 접근 시 "면제 절차(waiver)" 필요 가능성

- 한국은 위험 국가에는 속하지 않지만, 접근하고자 하는 기술이 DOE의 S&T Risk Matrix 상 Red 기술이라면 면제 절차 필요 가능성이 존재함을 유의

☑ Tip | 협력 주제가 Red 기술에 해당되는지 DOE 파트너와 함께 사전 검토 및 면제 필요 여부를 확인하고, 면제 필요시 관련 절차 절차에 맞춰 진행 권장

5. DOE 출장 규정은 우리나라가 아닌 DOE 관계자가 준수하는 사항임을 유의

- 민감주제 또는 민감국가, 발표자료 및 기술자료 사전 검토 등 DOE 출장 규정은 우리나라가 아닌 DOE 관계자가 준수하는 사항이므로 우리나라 측에서 DOE 및 국립연구소 관계자 등에게 선제적으로 안내 또는 요청을 할 필요는 없음을 유의
- 특히, DOE 산하 국립연구소별로 세부 출장 규정 및 관리 수준 등이 상이할 수 있다는 점을 인지

☑ Tip | 관련 내용을 인지만 하되, 필요시 증빙 등을 위한 요청이 올 경우 협조

그래도 궁금해요! DOE 사업에 참여하고자 하는 연구자를 위한 FAQ

※ (참고) 관련 상세 규정 및 연구보안 관리 수준은 개별 국립연구소마다 다를 수 있음

| 표 4 | DOE O 486.1A 및 DOE O 142.3B 관련 FAQ

질문	설명	대응방안
과거 위험국가의 FGTRP에 참여한 이력이 있습니다. DOE와 CRADA를 체결하여 협력할 수 있나요?	CRADA 규정에 FGTRP에 대한 직접 언급은 없으므로 CRADA 체결 시 FGTRP 이력을 요청하는 절차가 있는 경우는 드물고 대신 FOCI(외국 영향력) 심사를 거치지만, DOE O 486.1A 규정에 의거하여 FGTRP 이력을 요구할 가능성 존재	DOE 또는 국립연구소 측에서 FGTRP 관련 정보 요청을 할 경우, 연구자들의 관련 이력을 사전에 준비하는 것을 권장
DOE 연구소를 방문하려면 어떤 절차를 거쳐야 하나요?	DOE 시설에 접근하려면 FACTS에 신원 등록 및 호스트의 사전 승인 필요하며, FACTS 신원 등록은 DOE 담당자가 수행 ※ 구체적 절차는 개별 국립연구소마다 상이할 수 있으며, 장기 체류의 경우 FNAP(Foreign National Access Program) 등록 양식을 연구자에게 기입 요청하기도 함	DOE 또는 국립연구소 파트너(예 : 국립연구소 PI 등)에게 방문 요청 후 안내받은 절차(예 : FNAP 등)를 통해 해당 연구소 담당 직원이 방문자의 신원을 FACTS 등록 및 호스트 승인 절차를 거쳐야 함 ※ 구체적 절차는 개별 국립연구소별로 상이할 수 있음
DOE와 협력하려면 사전 제출해야 할 서류가 있나요?	이력서, 방문 목적 설명서, 체류 신분 등 상세 정보를 사전에 제출	DOE 또는 국립연구소 기준에 맞춘 이력서 및 방문계획서를 준비하고, 제출 시점도 미리 확인
DOE 또는 국립연구소 방문 시 미국 호스트가 꼭 필요하나요?	DOE 또는 국립연구소 호스트가 외국인을 초청하고 책임지는 절차가 필수로 요구	신원이 보장된 DOE 또는 국립연구소 직원 등 명확한 호스트 사전 확보 필요
DOE와 공동연구에 참여하면서 미국 체류를 하려면 비자가 꼭 필요한가요?	미국 내 체류를 수반할 경우 유효한 비자와 체류 신분 증명이 반드시 필요	방문 또는 체류 목적에 맞는 비자 종류(F, J, B 등)를 확인하고 사전 신청
방문 목적이 명확하지 않거나 애매할 경우 승인받을 수 있나요?	원칙상 방문 목적이 불명확할 경우 DOE는 승인을 거부하거나 심사를 보류할 수 있음	DOE 또는 국립연구소 측에 방문 목적을 명확히 설명하고, 필요 시 설명서를 첨부
SST(테러지원국) 국적자와 함께 협력하면 문제가 되나요?	SST 국적자와의 공동연구 또는 동반 시 DOE HQ 및 정보기관의 특별 심사 대상이 될 수 있음	협력자가 SST 국적자인 경우 DOE에 반드시 사전 고지하고 검토를 요청

2 사업·기술 기반 관리

관련 DOE 규정

- **과학기술 위험 분류 매트릭스 :** Science & Technology (S&T) Risk Matrix ('22.12.17.)
- **국립연구소의 외국기관과의 협력지침 :** DOE P 485.1A (Foreign Engagements with DOE National Laboratories, 2022.10.7.)
- **협동연구개발계약(CRADA) :** DOE O 483.1B Chg 2 (Cooperative Research and Development Agreements, 2020.10.21.)
- **전략적 파트너십 프로그램(SPP) :** DOE O 481.1E Chg 1 (Strategic Partnership Projects, 2022.3.4.)

1) 신흥기술의 위험 등급 분류 및 별도 보안관리 조치

※ (관련 규정) **Science & Technology (S&T) Risk Matrix**

- DOE는 기존의 수출통제나 분류 체계에 포함되지 않는 신흥기술이라 하더라도, 국가안보 또는 경제안보에 잠재적 위험이 있다고 판단되는 기술을 식별하고 보호하기 위해 S&T Risk Matrix를 운용

- 이 매트릭스는 기존 수출통제 제도(ITAR, EAR)로 보호되지 않는 기술까지 포함하여, **3단계 등급(Red, Yellow, Green)으로 민감도를 구분**함

| 표 5 | Red, Yellow, Green 기술등급 정의 및 조치

등급	정의	조치
Red	미국의 경제적 또는 국제 경쟁력과 관련된 민감성을 내포하고 있으며, 이러한 기술이 적절한 심사와 승인 없이 '위험국가(Country of Risk)'에 공유될 경우, 미국의 핵심 국가 이익에 중대한 피해를 초래할 수 있는 신흥 기술 주제	• "제한 기술(restricted)"로 분류 • 위험국가 소속자 또는 기관의 접근은 DOE 본부(HQ) 및 현장 기관(field)의 강화된 심사 및 사전 승인을 필수로 요구
Yellow	경제적 또는 국제 경쟁력 관점에서 향후 Red(제한 기술)로 지정될 가능성이 있거나, 강화된 주의가 요구되는 신흥 기술 주제	• 강화된 모니터링 필요 • 위험국가 또는 외국인의 접근 시, 조건부 승인 또는 면제 절차 적용 가능성 있음
Green	경제적 또는 국제 경쟁력과 관련된 특별한 민감성이 없는 신흥 기술 주제	• 별도 제한 없음 • 일반적인 국제공동연구 및 협력 가능

① Red

- **경제적·국제적 경쟁력과 관련된 민감성**을 가지며, 이러한 기술이 **적절한 심사 및 승인 없이 위험국가(Country of Risk)에 공유될 경우, 미국의 핵심 국가이익에 중대한 피해**를 초래할 수 있는 신흥 기술 주제
- 이러한 Red 주제들은 다양한 DOE 명령(DOE Orders)에서 정의된 바와 같이, 위험국 또는 그 소속자와의 상호작용과 관련하여 강화된 심사 및 통제를 적용받는 **"제한 기술(restricted)"로 간주됨**
- Red 기술에 접근하려는 위험국가 소속 개인 또는 기관은 DOE 본부(HQ) 및 현장 기관(Field) 양측에서 강화된 심사와 승인을 받아야 함
- DOE 산하 연구소는 다음을 포함하는 **접근관리계획(Access Management Plan)**을 수립하고, **프로젝트**

수명주기 전반에 걸쳐 적절한 보호가 이루어지도록 정기적 감독 및 모니터링을 수행해야 함 :

1. 제한으로 분류된 연구의 세부 설명
2. 책임 있는 주요 연구책임자(Principal Investigator)
3. DOE O 471.7(Controlled Unclassified Information, CUI)에 정의된 바에 따라, 제한 기술에 대한 물리적, 논리적, 행정적 접근 통제 절차
4. 해당 기술의 지식재산권(IP) 보호 조치 및 공개 또는 출판 전에 관련자에게 적절히 통지하는 절차
5. 미국 내에서라도 Export License 없이 정보 공유 불가 (Deemed Export)
6. DOE O 241.1B는 과학기술정보(Scientific and Technical Information, STI)를 적절히 식별·분류·배포·보존하는 절차를 규정하며, 이의 세부 요구사항은 계약자 요구문서(CRD)에 명시되어 있음. 각 연구소는 CRD에 따라 자체 절차를 마련하고, 이 절차에는 제한 기술 주제에 대한 적절한 검토 및 승인 절차가 반드시 포함되어야 함

② Yellow

- **경제적·국제 경쟁력** 측면에서 **향후 Red(제한 기술)로 지정될 가능성이 있거나, 강화된 주의가 필요한 분야**에 해당하는 신흥 기술 주제를 의미
- Yellow 기술 주제에 대해서는 다음과 같은 **보호조치** 가능 :

1. Yellow 등급 기술 주제는 특정 상황에서 추가적인 통제 조치가 요구될 수 있음
2. Yellow 주제는 일종의 "관심 목록(watch list)"에 해당한다고 이해할 수 있으며, 각 연구소는 Yellow 기술에 대한 모니터링 및 통제 체계를 자체적으로 마련해야 함
3. 기술 분야에 따라 Yellow 기술은 명확한 기술적 기준에 의해 정의될 수도 있고, 또는 기술/보안 분야 전문가(SME)의 판단을 필요로 할 수도 있음
4. 연구소는 필요 시 Red 등급 기술에 요구되는 접근관리계획(Access Management Plan)의 요소를 참고하여 Yellow 등급 기술 프로젝트에 대한 접근계획을 수립할 수 있음
5. 가능하면 기존의 보호조치 또는 프로그램을 활용하여 해당 프로젝트에 필요한 통제조치를 적용하는 것이 바람직
6. Yellow 주제의 경우, 위험국(Country of Risk) 출신 인물과의 정보 공유나 공동 활동과 관련하여 연구자 및 관리자에게 별도의 교육 또는 인식 제고 프로그램(coaching/awareness training)이 요구될 수 있음

③ Green

- 경제적 및/또는 국제 경쟁력과 관련된 **특별한 민감성이 없는 신흥 기술 주제**를 의미함.
- 기초 과학 연구나 기술 성숙도 수준(Technology Readiness Level, TRL)이 낮은 기술은 일반적으로 Green 등급에 해당하지만, 반드시 그런 것은 아님
- Green 등급 기술은 기존에 마련된 통제체계 외에 추가적인 보호조치가 요구되지 않으며, 현재 운용 중인 관리 체계에 따라 처리됨

2) DOE 및 산하 국립연구소의 외국기관과의 협력 지침

※ (관련 규정) **외국기관과의 협력지침 :** DOE P 485.1A (Foreign Engagements with DOE National Laboratories, 2022.10.7.)

– **(검토 사항)** DOE는 외국 기관과의 협력이 DOE 및 연구소의 미션과 정합되고, 연구소의 주요 임무 수행에 방해가

되지 않아야 한다는 요건을 제시하며, 외국 기관과의 협력 시 **다음 조건을 충족하는지 여부를 검토**

- 미국의 전략적 이익 및 외교 정책과의 일치 여부
- 미국 법령 및 규정 준수 여부 (예 : ITAR, EAR, 10 CFR Part 810 등)
- 국가정보 및 안보 관련 고려사항 반영 여부
- DOE 연구 및 기술 공유에 따른 리스크 평가 포함 여부

– **(검토 대상 협력)** 이러한 검토 범위는 ①양해각서(MOU) 및 유사 문서 (LOI, Statement of Intent 등), ②전략적 파트너십 프로그램(SPP, 구 Work for Others), ③협동연구개발계약(CRADA), ④기술상용화 협정(ACT), ⑤기타 외국 기관과의 계약적 법적 문서 등에 적용

※ 협동연구개발계약(CRADA), 전략적 파트너십 프로그램(SPP)은 **후술할 별도의 규정 운영 중**

– **(검토 절차)** 모든 협력안은 **DOE 본부 차원의 사전 검토***를 거치며, 모든 MOU 및 계약 문서는 **최소 5년마다 본부에서 재검토**하여 **정책 및 국가안보 기준과 일치 여부**를 확인하므로 유의

* CSO (Cognizant Secretarial Office), PSO (Program Secretarial Office), DOE 국제협력국(IA), 법무실(GC), 정보보안/국가정보국(IN), 비확산 담당 부서(NA-20), 분류정보 담당 부서(AU-60, 필요시)의 검토 수행

– **(제한 사항)** S&T Risk Matrix에서 제한(restricted) 기술로 지정된 분야(예 : Red 기술)에 대해, 위험국가(Countries of Risk)와의 협력은 사전 면제*가 없는 한 금지됨.

* 면제 요청은 현장 책임 부서(Field Element)가 연구소와 협의하여 제출 가능하며, FOAB(Federal Oversight Advisory Body)의 검토를 거쳐 관련 차관(Under Secretary)의 최종 승인 필요

3) 협동연구개발계약(CRADA) 체결 시 외국기관 참여 요건

※ (관련 규정) **DOE O 483.1B Chg 2**

– **(승인 요건)** DOE는 외국 기관과의 CRADA 체결 시 다음과 같은 요건을 제시하므로 해당 요건에 부합하는지 여부를 사전에 검토 필요

- DOE의 프로그램 및 시설 미션과 일치해야 하며, 민간 참여자는 단순 자금 제공이 아니라 실질적 기술 협력에 기여해야 함
- 미국 내 기술 활용 우선 조건(U.S. Competitiveness Clause)을 충족해야 함
- 수출통제, 기밀정보, 지식재산권(IP) 관련 보호조치가 명시되어야 하며, 필요한 경우 최대 5년간 보호 가능
- 참여기관이 외국 소유·지배·영향(FOCI)을 받는 경우, FOCI 검토를 통과해야 함

– **(승인 관련 조치)** 외국 기관이 참여하는 경우 DOE는 다음과 같은 조치가 가능하므로 유의

- 자금 출처 확인 (미국 정부 자금일 경우 특별 검토)
- 지식재산권(IP) 권리 명확화
- DOE 및 계약기관이 CRADA 참여자의 FOCI(외국 소유·지배·영향 여부) 검토 가능

– **(승인 관련 추가 절차)** 해당 협력이 위험국가 소속 외국 기관과의 협력이거나, S&T Risk Matrix 상의 제한 기술 분야에 해당하는 경우 :

- DOE 현장(Field Element)은 사전 심사를 통해 Red 기술 여부를 검토.
- Red 기술로 확인되면, 면제 요청서(exemption request)를 작성하여 CSO, PSO, FOAB를 거쳐 Under Secretary의 최종 승인을 받아야 함

4) 전략적 파트너십 프로그램 (Strategic Partnership Projects, SPP) 승인 요건

※ (관련 규정) 전략적 파트너십 프로그램 : DOE O 481.1E Chg 1 (Strategic Partnership Projects, SPP)

- **(정의)** DOE 또는 NNSA(National Nuclear Security Administration, 국립핵안보청) 시설이 외부 기관(미국 내·외 정부, 산업계, 학계 등)의 자금을 받아 연구·기술·서비스를 제공하는 제도로, DOE 예산이 아닌 외부 자금으로 수행되는 연구·기술 프로젝트
- **(목적)** 민간에서 수행하기 어려운 특수한 기술/시설 활용 제공, DOE 기술의 산업 이전 및 상업화 촉진, DOE/NNSA 연구소의 기술 기반 강화, 정부기관 간 협력 또는 민간과의 공동 연구 활성화
- **(SPP 승인 요건)** SPP 체결 시 충족해야 하는 조건은 다음과 같음
  - 협력 과제는 **DOE 또는 NNSA의 미션과 일치하거나 이를 보완**하는 것이어야 하며, 해당 연구소의 **기존 프로그램에 부정적 영향을 주지 않아야 함**
  - SPP는 **미국 민간 부문과의 직접적인 경쟁을 유발해서는 안 됨**
  - 과도한 리소스 소모 또는 **미래에 부담이 될 가능성이 없어야 함**
  - 모든 DOE **지침, 보안, 수출통제, 환경 규정을 철저히 준수**해야 함
  - **위험국가**는 제안된 기술이 S&T Risk Matrix상 Red 기술에 해당하는 경우, **반드시 FOAB의 심사 및 DOE Under Secretary의 승인을 받아야 함**

참고 S&T Risk Matrix 기술 분류 예시 ('22.12.17. 분류 기준)

① Quantum Information Science & Technology (양자정보과학기술)

※ 아래 기술들은 기밀정보, 수출통제, NDA(비공개 계약) 등에 의해 이미 보호되는 경우가 있으며, 공개 전에는 개별 사례별로 규제 적용 여부를 검토해야 함.

(1) 컴퓨팅 및 시뮬레이션 (Computing and Simulation)

등급	예시 기술
Yellow	• NISQ 이후 시대를 위한 고정밀 큐비트 기술 개발 • 고대역폭 및 극저온 제어 기술 • 오류 완화 기술 및 로직 큐비트 개발 • 오류 수정 코드 부분 실행 실험 • 50~100 큐비트 실험 장치 • 4.2K 이하에서 장시간 동작 가능한 대형 냉동기 • 향후 양자컴퓨팅 기술 구현 로드맵 작성 • 오류 수정 없이는 결함 허용 불가한 큐비트 시연
Green	• 양자역학과 정보이론의 기초 원리 탐구 • 새로운 큐비트 기술 개념 • 환경이 큐비트 성능에 미치는 영향 분석 • 고대역폭 제어용 실온 전자장치 • 양자 무작위 수 생성기 개발 • 디지털/아날로그 양자 시뮬레이션 • 화학/물리/AI용 양자 알고리즘 개발 • NISQ 장치 운영용 소프트웨어 • 아키텍처 중립적 오류 수정 기초연구

(2) 센싱, 시계, 계측 (Sensing, Clocks, and Metrology)

등급	예시 기술
Yellow	• 얽힘 광자 기반 원거리 이미징 기술 • 정확도 ps/day를 초과하는 양자 시계 개발 • 100m 오차 수준의 양자 항법 시스템 • 현장 적용 가능한 양자 센서용 시스템 구성요소 개발
Green	• 기초연구 목적의 일반적인 양자 센싱 • 원자 시계 및 네트워크 시계에 대한 연구 • 양자 기반 고해상도 실험용 현미경

(3) 통신 (Communication)

등급	예시 기술
Yellow	• 실용적 속도로 얽힘 전송을 안정적으로 수행하는 기술 • 양자 키 분배 외의 양자 사이버보안 기술 • 양자 반복기를 활용한 오류 수정 기반 양자 통신 실험 • 다자간 또는 다노드 얽힘 전송 시연
Green	• 양자 네트워크 기본 구성요소 개발 (단일/얽힘 광자 소스, 검출기, 양자 메모리 등) • 양자 반복기(Quantum Repeater) 기초연구 • 기초과학 또는 센싱 응용 목적의 양자 네트워크 사례 연구

(4) 재료 및 제작 (Materials and Fabrication)

등급	예시 기술
Yellow	• 공정 제어 없이 큐비트 생산 수율을 향상시키는 실험 기술 • QIST에 관련된 재료에 대한 동위원소 농축 기술 개발 • 양자 디바이스 성능 예측용 재료 모델링 기술 • 마요라나 모드 조작이 가능한 위상 양자재료 연구 • 양자컴퓨터용 농축 안정 동위원소 연구 • 미세한 공정 기술 요소 개발 (원자 트랩, 리소그래피 등) • NISQ 이후 시대를 위한 신소재 기반 양자 디바이스 평가 기술
Green	• 밀리켈빈 온도에서 양자재료/큐비트 재료 연구 • 2차원 위상재료·그래핀 나노리본 등 양자 디바이스용 재료 탐색 • 양자재료의 속성을 빠르게 평가할 수 있는 실험 기술 개발

② High Performance Computing (고성능컴퓨팅)

※ 주의 : HPC 기술이 다른 분야의 연구에 활용될 경우, 해당 분야의 가이드라인을 따라야 하며, HPC 자체 기준은 적용되지 않음

※ 이미 기밀, 수출통제, NDA(비공개 계약) 하에 보호되고 있는 정보는 아래 내용에 포함되지 않음. 기술 공개 또는 활용 전 사례별로 규제 준수 여부를 반드시 검토해야 함

(1) HPC 시스템 R&D

등급	예시 기술
Yellow	• 현재까지 식별된 항목 없음 (다만 일부는 수출통제 또는 기밀로 보호 중)
Green	• 특정 시스템과 무관한 일반 R&D (예 : 복원력, 에너지 효율 관련 시스템 관리 연구, 시스템 상태 감시 및 성능 네트워크와 런타임 소프트웨어 통합 연구 등)

(2) 벤더 하드웨어 구성요소(공동 설계 포함)

등급	예시 기술
Yellow	• 제품 설계에 반영되지 않은 공동설계 제안 사항 • 제품 설계 반영 전의 공동설계 제안 ※ 사전 공개되지 않은 성능 데이터는 NDA로 보호되어야 함
Green	• NDA에 해당하지 않는 사후 공개된 설계 정보 • 공개된 프로세서 아키텍처(ISA), 성능 특성 • 메모리/저장장치 성능, 인터페이스 • 사용자 수준 네트워크 프로그래밍 인터페이스

(3) HPC 시스템 구성요소 및 기술에 대한 연구

등급	예시 기술
Yellow	• 제조 전이지만 설계도를 통해 복제 가능한 상세 설계 • DOE 또는 미 정부 활용 가치가 있어 특허 전 단계의 기술
Green	• HPC 시스템 또는 센서의 개념 설계 • 이와 관련된 예측, 모델링, 분석 등 • 특허로 등록된 연구소 기술 성과

(4) HPC 시스템 소프트웨어

등급	예시 기술
Yellow	• 현재까지 식별된 항목 없음 (단, 일부는 보호 조치 중)
Green	• 연구소가 개발한 범용 시스템 소프트웨어 • 연구소가 사용하거나 수정한 오픈소스 시스템 소프트웨어

(5) HPC 응용 라이브러리 및 프레임워크

등급	예시 기술
Yellow	• 수출통제, 기밀, 지식재산권, 타 기술 분야 또는 타 통제 대상 애플리케이션에 특화된 모듈
Green	• 오픈소스 라이브러리 및 프레임워크

③ Machine Learning / Artificial Intelligence (기계학습 / 인공지능)

※ 아래 내용은 이미 기밀 지정, 수출통제, 비공개 계약(NDA) 등에 의해 보호되는 정보는 포함하지 않음

※ 정보 공개 전에는 사례별로 해당 규제와의 관련성을 반드시 검토해야 함

(1) 기초 알고리즘 및 기초 연구 (Foundational Algorithms and Basic Research)

등급	예시 기술
Yellow	• Yellow 등급 데이터에 기반한 학습 결과물은 자동으로 Yellow로 간주됨 (데이터가 Yellow → 결과도 Yellow)
Green	• ML 알고리즘 및 방법론에 대한 기초 연구 • 시뮬레이션과 머신러닝 결합 방법 연구

(2) 제어 시스템 관련 연구 (Controls)

등급	예시 기술
Yellow	• 네트워크 격리와 중요 인프라 모니터링을 포함하는 보안 다중 계층 제어 시스템 • NIST/FISMA 기준을 적용한 기술·관리 통제 조치 • 연례 감사 및 테스트 대상 보안 시스템
Green	• AI/ML을 활용한 제어 시스템의 기초 연구

(3) 사회 응용 분야 (Societal Applications)

등급	예시 기술
Yellow	• 생체인식(Biometrics) 또는 얼굴인식(Facial recognition)을 포함한 응용
Green	• 데이터 프라이버시 향상을 위한 ML/AI 기술 • 보건 응용 분야 : – 신약 설계 – 질병 탐지 및 분류 – 치료/개입/개인맞춤 의학 – 프라이버시 기초 연구

(4) 국가안보 응용 (National Security)

등급	예시 기술
Yellow	• 사이버 보안용 AI/ML 기술 (공격 은폐용 정상 활동 모방 등) • 역AI 기술 : – 분류기의 적대적 입력 탐지 – 학습데이터 특성 추론용 역공학 기법 – 모델 보호 또는 악용 기법 • 학습 데이터 조작, 결정경계 왜곡 기법 • 문서 분류 자동화 • 생성형 AI를 통한 콘텐츠 생성 및 검토 기술 (Red에 포함되지 않은 경우)
Green	• 에지(edge) 환경에서의 ML 알고리즘 보안 연구

(5) 에너지 분야 응용 (Energy)

등급	예시 기술
Yellow	• 현재까지 보호 조치 외에 별도로 식별된 Yellow 항목 없음
Green	• 자율형 에너지 시스템 • 분자 설계 • 에너지 예측용 알고리즘 개발 • 지하 시스템 거동 분석 • 자동 특성 식별 및 고해상도 데이터 생성/활용 기법

④ **Battery Science & Technology (배터리 과학기술)**

※ 아래 항목에는 이미 기밀, 수출통제, NDA(비공개 계약) 등에 의해 보호되는 정보는 포함되어 있지 않음

※ 정보의 공개 또는 활용 전에 사례별로 적절한 규제와의 관련성을 반드시 확인해야 함

- 항상 Green으로 간주되는 항목
  1. 분석/진단/측정 기법 및 해당 도구의 연구 개발
  2. 기초 연구 수준의 시뮬레이션/계산 도구
  3. 신규 소재 고속 탐색(high throughput discovery)
  4. 기초 수준의 반응 메커니즘, 구조-물성 관계 연구

(1) 양극(Cathodes)

등급	예시 기술
Yellow	200mAh/g 이상 용량 또는 2.0~4.5V 동작 가능성이 있는 상용 양극재의 수정·분석
Green	상용 양극재의 열화/고장 메커니즘 분석

(2) 음극(Anodes)

등급	예시 기술
Yellow	용량이 1000mAh/cm^3 이상인 상용 음극재의 수정·분석
Green	상용 음극재의 열화/고장 메커니즘 분석

(3) 리튬(Lithium)

등급	예시 기술
Yellow	스트리핑·도금 안정화 및 고체전해질 계면 안정화 연구
Green	Li 금속 음극 관련 기초 고장 메커니즘 이해

(4) 고체 전해질

등급	예시 기술
Yellow	계면 안정화 기술 개발 및 수정 연구
Green	기존 고체전해질의 화학적·물리적 특성 분석

(5) 충전 속도

등급	예시 기술
Yellow	10분 이내 2.5mAh/cm^2 이상 수용 가능한 빠른 충전 기술
Green	고속 충전이 셀 성능·수명에 미치는 영향 연구

(6) 에너지 저장

등급	예시 기술
Yellow	설치비 $200/kWh 이하 달성 가능한 고정형 저장 기술 또는 제조비 $80/kWh 이하 달성 기술
Green	개념 단계의 에너지 저장 시스템 연구

(7) 재활용

등급	예시 기술
Yellow	정제 없이 양극 제조 공정에 직접 투입 가능한 재활용 제품 생성 방식
Green	배터리 등급 미만의 금속 회수 방식

(8) 열폭주(Thermal Runaway)

등급	예시 기술
Yellow	열폭주 상황(과전압, 온도상승 등)에서도 셀 간 전파를 방지할 수 있는 기술
Green	개념 수준의 열폭주 대응 시스템

(9) 수명(Lifetime)

등급	예시 기술
Yellow	실험 데이터 없이도 특정 열화 메커니즘을 분류할 수 있는 범용 추정 방식, ML 기반 소재 탐색 초기 연구 포함
Green	셀 설계 없이 상용 셀 대상 단순 열화 추정 방식

(10) 기술경제성(Technoeconomics)

등급	예시 기술
Yellow	현재까지는 별도로 식별된 Yellow 항목 없음
Green	에너지 저장 구성품·시스템에 대한 생애주기 및 경제성 평가

⑤ Bioscience & Biotechnology (생명과학 및 생명공학)

※ 기밀정보, 수출통제정보, 비공개 계약정보(NDA) 등은 제외하며, 정보 공개·배포 전 별도 검토 필요

(1) 합성생물학 (Synthetic Biology)

등급	예시 기술
Yellow	• 합성생물학 기술을 이용한 바이오연료 생산용 상업화 최적화 • 민감국가에서 입수 불가능한 장비 또는 시약 • 유전체 크기 증가, 바이러스 전달효율 향상 등 전략 기술 발전이 포함된 경우 • 합성 바이러스 부활(rescue), 유전자 구동 기술 등
Green	• GenBank, DIVA 등 공개 DNA/단백질 정보 DB 사용 • 비병원성 균주에 대한 기초연구 목적의 유전자 조작 • 유전자 발현 조절을 위한 dCas9 등 기초도구 사용

(2) 오믹스 및 자동화 기술 (Omics & Automation Technologies)

등급	예시 기술
Yellow	• 전장 유전체 시퀀싱 센터 보호 대책 개발 • 오믹스 자동화 장비의 오용 방지 시스템 • 국방/정보목적의 실시간 측정 가능한 오믹스 장비 • 인간개입 없이 생체샘플을 자동으로 처리하는 시스템
Green	• 공개 기술 기반 기초 연구 • 복수의 분석장비를 조합한 표준 연구 • 단일 오믹스 측정 또는 메커니즘 분석용

(3) 데이터 및 고급 계산생물학 (Data & Advanced Computational Biology)

등급	예시 기술
Yellow	• 미국 상무부 수출통제목록 대상 생물정보 DB 가공 • 클라우드 생물데이터 보안 체계 개발 • MCM 예측모델용 통제된 데이터셋 활용 • 비공개 유전체 검색 소프트웨어/워크플로우, 생물학적 위협인자 탐지 시스템
Green	• 공개 데이터 기반 계산생물학 연구 • 기초 메커니즘 규명 목적의 모델링/시뮬레이션

(4) 바이오제조 및 바이오소재 (Biomanufacturing & Biomaterials)

등급	예시 기술
Yellow	• 국가안보 또는 전략 산업에 필수적인 상용화 목적 미생물 경로 최적화 • 희토류 채굴용 유전자 조작 미생물 개발 • 상업 규모의 추출 및 정제 공정 • 다효소반응을 위한 효소 고정화 또는 서브스트레이트 채널링 기술
Green	• 기초적 단백질 발현 시스템 및 배양 기술 • 조직 수준의 공정 및 추출기술 • 공정 시뮬레이션 및 진단 기술

(5) 농업 및 환경기술 (Agricultural & Environmental Technologies)

등급	예시 기술
Yellow	• 필드시험 기반 전환기술 검증 • 고효율 작물 전환기술의 파일럿 규모 적용 • 바이오에너지작물 처리 기술의 파일럿 개발
Green	• 공개된 germplasm 기반 유전자-형질 연구 • 마커기반 육종 및 실험실 기반 유전체 분석 • 수직농장, 식물 마이크로바이옴, 3D 프린팅 식품 연구 등

(6) 생의학 연구 및 기술 (Biomedical Research & Technologies)

등급	예시 기술
Yellow	• 인체 내 전달 시스템 개발 (예 : 나노소재, 뇌혈관 장벽 통과) • 혈액 대체물 또는 조직 재생물질의 고기능화 • 신경공학 기술, 뇌파 기반 인터페이스(BCI) 연구 • 산업 수준 의약품 공정 설계 및 최적화
Green	• 세포 메커니즘, 방사선 반응 등 생물학적 기초 연구 • 바이오이미징, 유전체 분석을 포함한 진단도구 개발 • AI 기반 임상 최적화 시스템

⑥ Accelerator Science & Technology (가속기 과학기술)

※ 타 분야의 과학기술 개발에 가속기 기술이 기여할 경우, 해당 분야의 S&T 위험 매트릭스 가이드를 따라 제한 여부 판단이 필요함

※ 이미 분류(Classification) 또는 수출통제(Export Control), 혹은 공급사 NDA로 보호되는 정보는 본 매트릭스에 포함되지 않으며, 공개 전 사안별로 통제 여부를 별도로 평가해야 함

(1) 초전도 라디오 주파수(Superconducting Radio Frequency, SRF) 기술

등급	예시 기술
Yellow	• 고 Q값 또는 고 그라디언트를 가진 크라이오모듈 개발 (예 : 1300 MHz, 50 MV/m 이상 등) • 산업·의료·안보 응용을 위한 전도 냉각형 SRF 시스템 개발 • 좁은 주파수 대역폭에 맞춘 공명 제어 기술 개발
Green	• 기본 연구용 SRF 가속기 설계 및 활용 • 희귀 동위원소 연구, 중성미자 시설, 미래의 고에너지/핵 물리 콜라이더 등에서 사용 예정인 가속기에 대한 일반적인 SRF 연구 • 나이오븀 표면 처리, 새로운 재료 및 코팅 기술 관련 연구 (특정 프로젝트와 무관할 경우) • 청정실 조립기술, 공통적 크라이오모듈 설계기술 등 • 4K 이상의 온도에서 전도 냉각되는 SRF 시스템 개발

(2) 레이저 및 플라즈마 웨이크필드 가속기 기술

등급	예시 기술
Yellow	• 실험실 단계를 넘은 통합 시스템으로 5년 이내 시장 가능성 있는 경우 • 고에너지 물리 콜라이더, MeV 광자 소스, 자유전자 레이저 등 응용 가능성 높은 시스템
Green	• 기본 연구용 플라즈마 가스 밸브, 레이저 이온화 시스템 등 (상용 부품 기반) • 물리 개념 수준의 입자 주입·빔 제어 기술 • 방사선 진단 기술 개발

(3) 초전도 자석 기술

등급	예시 기술
Yellow	• 고온 초전도체(〉10K), 고임계자기장(〉15T) 재료 개발 • 12T 이상 고자기장 자석 기술(상업용 응용 전제) • 비공개 설계도구 및 고급 시뮬레이션 기법
Green	• 기본 연구 목적의 자석 설계 및 피드백 분석 • NbTi 자석 제작기술 개발 • 기초과학용 고자기장 자석 개발

(4) 극저온 플랜트 설계 및 운영

등급	예시 기술
Yellow	• 해당 없음 (현재는 별도 제한 없음)
Green	• 저온에서의 재료 물성 연구 • 극저온 장비 최적화 설계

(5) 첨단 광원 기술

등급	예시 기술
Yellow	• 특정 프로젝트 적용을 위한 통합 설계 구현 • FEL(자유전자 레이저) 최적화용 신형 광전자 음극 개발 • 차세대 초전도 언듈레이터 개발 등
Green	• 기본 연구 및 장기 개발 중인 기술 • 초고속 펄스 전자기기, 저장 링 일반 설계, 비선형 광학 등 • 전자 빔 위치 모니터 등 고정밀 진단기기 개발

(6) 고전류 전자/하드론 빔 기술

등급	예시 기술
Yellow	• 5~10 MW급 고출력 양성자 빔 기술 • 자율 제어 시스템 설계, 머신러닝 기반 안정성 향상 연구 등
Green	• 에너지 회수형 선형가속기(ERL) 및 전자소스 관련 기본 연구 • 하드론(양성자 등) 빔 소스 연구 (중간 전류, 기본 밀도)

(7) 가속기 기반 핵시스템 및 동위원소 생산

등급	예시 기술
Yellow	• 해당 없음 (현재는 별도 제한 없음)
Green	• 기본 물리 연구 또는 핵분리 최적화 이전 단계의 방사화학 연구

Tip! **DOE와 공동연구를 계획 중인 연구자를 위한 상세 유의사항**

〈 S&T Risk Matrix 관련 유의사항 〉

1. Red 기술 포함 시 협력 절차가 강화됨

- Red 등급 기술은 “restricted topic”으로 간주되며, DOE는 위험국가(Country of Risk) 소속자뿐 아니라, 해당 기술의 민감도에 따라 제3국 연구자와의 협력에도 강화된 검토 절차를 적용할 수 있음
- 우리나라는 위험국가에 해당하지 않아 원칙적으로 위험국가에 준하는 강화된 제약을 받지는 않으나, 위험국가 국적자(예 : 포닥 등)가 참여연구원에 포함 시 심사가 강화될 수 있음
- 위험국가 여부와 무관하게 Red 기술에 포함된 민감한 정보 등에 따라 다음과 같은 조치가 요구될 수 있음 :
  - 해당 기술의 등급 분류에 관한 기술 설명서(technical narrative) 또는 분류 요청 문서 제출
  - DOE 본부의 Cognizant Secretarial Office(CSO) 또는 Program Secretarial Office(PSO)의 사전 승인
  - DOE 정보국(Office of Intelligence and Counterintelligence, IN)의 강화된 보안 심사(enhanced vetting)
  - CUI(Controlled Unclassified Information) 보호계획, 정보 보호 및 공개 제한 절차 수립

☑ **Tip |** DOE 또는 산하 국립연구소 측에서 Red 기술 관련 별도의 사항을 요청 시 조율

2. Yellow 기술은 사례에 따라 제한될 수 있음

- Yellow 기술은 향후 Red로 지정될 가능성이 있는 기술로, DOE는 특정 상황 또는 위험국가 소속자와의 협력 여부에 따라 추가 보호조치나 문서화된 통제계획 수립을 요구할 수 있음
- 개별 연구소 자체 판단에 따라 다음과 같은 조치가 적용될 수 있음 :
  - 자료 공유 범위 제한 또는 협력자별 정보 접근 제한
  - 논문, 발표자료에 대한 사전 검토 및 승인 절차
  - DOE 시설 내부 접근 제한(동행 조건 등) 또는 실험 장비 단독 사용 제한
  - Access Plan, Export Control 확인서, 인식제고 교육(Coaching/Awareness Training) 이수 등

☑ **Tip |** DOE 또는 산하 국립연구소 측에서 Yellow 기술 관련 별도의 사항을 요청 시 조율

3. 기술적 민감도는 다양한 협력 방식에도 영향을 미침

- S&T Risk Matrix는 연구 주제뿐 아니라, 해당 기술이 사용·공유되는 방식 전반에 걸쳐 위험도를 판단하므로 다음과 같은 요소들이 민감도 판단에 영향을 미칠 수 있음 :
  - 연구 수행 장소가 DOE 내부 시설인지 또는 외부 연구기관인지 여부
  - 실험 중 생성되거나 논문에 포함될 수 있는 민감 정보 또는 기술자료
  - 논문 공동저자에 위험국가 소속 연구자가 포함되는지 여부
  - DOE의 장비, 알고리즘, 데이터 또는 시뮬레이터 등의 사용 여부

☑ **Tip |** 협력 주제뿐만 아니라, 공동실험, 데이터 공유, 출판 등의 협력 방식 자체가 민감성 평가 대상이 될 수 있음을 유의하고, 필요시 사전에 협의해두는 것을 권장

4. S&T Risk Matrix는 다양한 DOE 정책들과 연계되어 적용됨

- DOE는 S&T Risk Matrix를 다음과 같은 주요 정책들과 연계하여 운용하고 있으며, 기술 등급에 따라 협력 승인 또는 제한 조치가 요구될 수 있음 :

정책	연계 방식
DOE O 142.3B	외국인의 DOE 시설 접근 및 협력 시, Red/Yellow 기술 포함 여부에 따라 추가 승인 또는 면제 필요
DOE O 483.1B	외국 기관과 CRADA 체결 전, S&T Risk Matrix 기반 기술 민감도 평가 수행
DOE O 481.1E	외국 기관과 SPP 체결 전, S&T Risk Matrix 기반 기술 민감도 평가 수행
DOE O 550.1	민감 기술이 포함된 DOE 직원의 해외출장 시, FTMS 등록 및 보안 관련 부서 사전 심사 연계
DOE P 485.1A	DOE의 대외 파트너십 활동 관리 시, S&T Risk Matrix를 통해 제한 기술 구분 및 대응 방안 수립

☑ Tip | DOE와의 협력 프로젝트는 위 정책의 적용을 받을 수 있음을 사전 인지하고 필요시 관련 사항 준비

〈 DOE 국립연구소와 국제공동연구 체결 시 공통 유의사항 〉

1. 협력 형식에 따라 사전 승인 필요

- 연구기관이 DOE 연구소와 아래 형식으로 협력하려면 DOE 본부(HQ)의 사전 검토 및 승인 필요
  - 양해각서(MOU, LOI 등), 전략적 파트너십 프로젝트(SPP), CRADA(공동연구개발협정), ACT(기술상용화 계약), 기타 외국 기관이 DOE 연구소에 연구를 요청하는 계약

☑ Tip | DOE는 사전 승인 없이 협의되거나 체결된 비공식 MOU를 인정하지 않으므로 정식 절차를 거쳐야 함

2. MOU 또는 계약 체결 시 DOE 본부 내 부서 검토 필요

- DOE가 외국 기관과 MOU를 체결하려면, 관련 부서(CSO, PSO, IA, GC, IN 등)의 사전 검토를 거쳐야 함

☑ Tip | DOE 측 파트너 기관이 내부 검토를 위해 요청할 수 있는 정보를 명확하고 신속하게 제공하는 것이 중요 (예 : 기관 정보, 공동 연구 목적, 기술 분야, 미국 내 기여 등)

3. S&T Risk Matrix 위험 분야 포함 여부 확인

- DOE는 위험 국가(Countries of Risk)와의 기술 협력을 제한하는 과학기술 위험 매트릭스(S&T Risk Matrix)을 운영
- 협력 주제가 S&T Risk Matrix 상 제한 기술(Red)로 분류된 경우, 위험국가 국적자와의 협력이 아니더라도 DOE 내부 정책에 따라 사전 면제 승인 절차를 밟도록 규정

☑ Tip | 우리나라는 위험국으로 분류되어 있지 않으나, 고위험 기술 분야에서의 협력은 필요 시 관련 절차를 준비

〈 CRADA 체결 시 유의사항 〉

1. DOE의 사명(Mission)에 부합해야 함

- 공동연구 주제는 DOE의 과학, 에너지, 안보 등의 미션과 관련되어야 하며, 우리나라 기관도 실질적으로 연구에 기여해야 한다는 요건을 제시(단순한 자금 지원은 인정되지 않음)

☑ Tip | 필요시 공동연구 목적이 DOE의 미션과 어떻게 연결되는지 기술할 것을 권장

2. 외국 기관 참여는 S&T Risk Matrix 사전 검토 대상

- DOE는 신흥 분야 관련, S&T Risk Matrix상 제한 기술에 해당할 경우 사전 승인 및 면제 요청 절차를 규정

☑ Tip | 우리나라는 위험 국가는 아니지만, 협력 기술이 제한 분야일 경우에는 면제 절차를 요청받을 수 있음

3. 미국 우선 조항(U.S. Competitiveness Clause) 적용 여부 등 지식재산권(IP) 및 데이터 권리 사전 협의 필요

- 공동 연구에서 생성되는 데이터/발명품에 대해 DOE는 미국 우선 사용권을 가지므로 한국 기관이 IP 공유 또는 상용화를 원할 경우 사전 협의 및 계약 명시 필요

☑ Tip | 우리나라 기관의 연구성과 활용(예 : 특허 출원, 제품화 등)을 희망한다면, 사전에 해당 내용을 CRADA에 명시

4. 자금 출처 및 소유 구조 정보 요구

- DOE는 CRADA 참여자의 자금 출처(국가 자금 여부), 소유·지배 구조(FOCI : Foreign Ownership, Control, or Influence)를 요청할 수 있음

☑ Tip | FOCI 관련 요청을 받을 경우 관련 정보를 투명하게 공개

5. CRADA 전 공동 작업 계획서(JWS) 제출 필수

- DOE에 제출할 Joint Work Statement에는 다음이 포함되어야 함 :
  - 연구 목적 및 범위, 참여 기관별 역할, 예상 산출물 및 일정, 민감 기술 여부 및 IP 분배 계획

☑ Tip | 필요시 사전에 미국 측 파트너와 조율하여 공동 작성 필요

〈 SPP 체결 시 유의사항 〉

1. SPP는 외국 기관도 참여 가능하나 사전 심사 필요

- DOE는 모든 외국 기관과의 SPP에 대해 보안, 기술, 외교적 관점에서 HQ 다부처 검토 실시

☑ Tip | DOE 측 파트너가 요구하는 문서(기관 개요, 자금 출처, 협력 목적 등) 준비

2. SPP 활동은 DOE의 사명과 부합해야 함

- SPP는 DOE의 과학·에너지·안보 미션을 지원하는 활동이어야 하며, 다음 조건을 충족해야 함 :
  - 협력 과제는 DOE 또는 NNSA의 미션과 일치하거나 이를 보완하는 것이어야 하며, 해당 연구소의 기존 프로그램에 부정적 영향을 주지 않아야 함
  - SPP는 미국 민간 부문과의 직접적인 경쟁을 유발해서는 안 됨
  - 과도한 리소스 소모 또는 미래에 부담이 될 가능성이 없어야 함
  - 모든 DOE 지침, 보안, 수출통제, 환경 규정을 철저히 준수해야 함
  - 위험국가는 제안된 기술이 S&T Risk Matrix상 Red 기술에 해당하는 경우, 반드시 FOAB의 심사 및 DOE Under Secretary의 승인을 받아야 함

☑ Tip | 필요시 공동연구 목적이 DOE의 미션과 어떻게 연결되는지 기술할 것을 권장

3. 미국 우선 조항(U.S. Competitiveness Clause) 적용 여부 등 지식재산권(IP) 및 데이터 권한 명확화

- SPP 결과물에 대해 DOE는 데이터 및 기술 보호 요건을 적용하며, 경우에 따라 미국 우선사용권이 적용되므로 우리나라가 지재권 확보나 상용화를 고려할 경우, 사전에 계약서에 명시해야 함

☑ Tip | 필요시 IP 및 데이터 권한 등에 대해 당사자 간 협의를 진행하고 이를 계약서에 명시 필요

그래도 궁금해요! DOE와 공동연구를 계획 중인 연구자를 위한 FAQ

※ (참고) 관련 상세 규정 및 연구보안 관리 수준은 개별 국립연구소마다 다를 수 있음

| 표 6 | S&T Risk Matrix 및 DOE P 485.1A 관련 FAQ

질문	설명	대응방안
우리 연구팀에 위험국가 국적의 포닥이 포함되어 있는 경우, DOE와 Red 기술 관련하여 DOE.O 485.1A에 명시된 협력(MOU, CRADA, SPP, ACT 등)이 가능한가요?	Red 기술은 위험국가 국적자와의 상호작용에 대해 강화된 심사 및 DOE 본부 승인 요건이 적용됨. 따라서 위험국가 국적의 포닥이 포함된 연구팀이 Red 기술 협력에 참여할 경우, 강화된 제한 및 승인 절차가 요구될 수 있음	협력 착수 전, DOE 또는 국립연구소 측에 기술 주제가 Red에 해당하는지 확인 위험국가 국적 포닥의 참여 여부를 명확히 밝히고, DOE 또는 국립연구소 측에 사전 협의 등 필요한 절차 요청 심사 소요 기간(보통 45일 이상)을 고려하여 일정 여유 확보 PI와 협력하여 접근관리계획(AMP) 포함 여부 확인 및 준비
Red 기술에 해당하면 DOE 협력이 불가능한가요?	기술 특성에 따라 협력이 불가능할 수 있고, 가능하더라도 별도의 보안 요구 발생 가능. 위험국가 국적자 포함 시 강화된 제한 및 승인 절차를 요구할 수 있음	DOE 또는 국립연구소 측에 해당 Red 기술의 기밀, 수출통제, CUI 포함 여부를 문의 후 협력 주제에 대한 적정성, 보안 요구사항, 정보 공개 범위에 대해 명확히 조율
Yellow 기술은 항상 제한되나요?	Yellow 기술은 기본적으로 모니터링 대상이며, 사례에 따라 일부 제한 또는 보안조치 요구 가능	DOE 또는 국립연구소 측에 해당 Yellow 기술의 보안관리 수준을 문의 후, 필요 시 협력 범위와 자료 공유 수준을 명확히 정리
우리 연구팀에 위험국가 국적의 포닥이 포함되어 있는 경우, DOE와 Yellow 기술 관련하여 DOE.O 485.1A에 명시된 협력(MOU, CRADA, SPP, ACT 등)이 가능한가요?	Yellow 기술에 위험국가 국적자가 포함될 경우, DOE 연구소는 자체 판단에 따라 정보 공유 제한, 역할 제한, 보안교육 등을 요구할 수 있음	해당 위험국가 국적 포닥의 역할을 사전에 명확히 구분하여 기술 민감도에 따라 참여 조정 DOE 또는 국립연구소 측과 참여 가능 범위 및 관리방안 사전 협의 권장
Green 기술은 자유롭게 협력 가능한가요?	Green 기술은 일반 협력, 정보 공유, 출판에 특별한 제약이 없음 따라서 일반적인 DOE 본부 검토 절차만 거치면 협력 가능하며 면제는 불필요	기초 연구, 공개 정보 중심으로 협력
기술 등급은 누가 판단하나요?	DOE 기술 담당자, 보안 담당자, 정보기관이 공동 판단	S&T Risk Matrix 상 기술 등급(Red/Yellow/Green)에 대한 분류 여부를 DOE 기술 담당자 또는 보안 담당자에게 확인 요청
기술 등급에 따라 어떤 추가 절차가 필요한가요?	기술 등급에 따라 DOE 본부 승인, 정보기관 심사, 보호계획 제출 등이 필요할 수 있음	프로젝트 개요, 기술 분류요청서, S&T 등급 판단 근거자료, 정보보호 관련 계획(CUI 등)을 사전 문서화해 준비

참고 DOE의 위험국가(Countries of Risk) 및 민감국가(Sensitive Countries) 관련 조치사항

1. 위험국가 정의 및 관련 조치

※ (근거 규정) DOE O 486.1A

- (위험국가 정의) 국가정보국장실(DNI)의 『세계 위협 평가(World Wide Threat Assessment)』 및 『미국 국가 방첩 전략(The National Counterintelligence Strategy of the United States of America)』 등을 고려하여, 과학차관이 에너지 차관, 핵안보 차관, 정보·방첩실과 협의한 후 지정한 위험 외국(foreign country of risk)을 의미함
- (위험국가 목록) 현재 DOE 지정 위험국가는 중국, 러시아, 이란, 북한, 벨라루스 5개국이며('25.5월 기준) 변동 가능

  ※ (근거) 美 DOE 홈페이지 (https : //www.energy.gov/science/countries-risk)
- (위험국가 관련 조치) DOE의 위험국가 관련 조치사항은 다음과 같음

| 표 7 | DOE의 위험국가(Countries of Risk) 관련 조치사항

주요 이슈	관련 규정	주요 조치사항
1. 제한기술 접근 관련 심사 강화	DOE O 142.3B	• 위험국가 국적자 또는 기관이 Red 등급 기술에 접근할 경우 DOE 본부 및 현장 차원의 심사 및 승인 강화
2. 위험국가 인재유치 프로그램 참여 금지	DOE O 486.1A	• DOE 직원 및 Contractor Personnel의 위험국가의 외국 정부 후원 인재 유치 프로그램(FGTRP)에 참여 금지 • DOE 직원 및 고용 관계가 있는 Contractor Employee의 위험국가의 기타 외국 정부 후원 또는 연계 활동(Other Foreign Government Sponsored or Affiliated Activities)에 대한 참여도 제한
3. 국립연구소와 위험국가 간 제한기술 협력 금지	DOE P 485.1A	• DOE 국립연구소는 위험국가와 S&T Risk Matrix상 Red 기술이 포함된 협력(MOU, CRADA, SPP 등)을 수행할 수 없으며, 수행을 위해서는 FOAB 검토 및 DOE 차관 사전 면제 승인 필요
4. CRADA 제한	DOE O 483.1B	• 위험국가 기관과 CRADA 체결 추진 시 해당 기술이 S&T Risk Matrix 상 Red 분야인 경우 FOAB을 통해 관할 차관 또는 지정자의 사전 예외 승인 필요
5. SPP 제한	DOE O 481.1E	• 위험국가 기관과 SPP 체결 추진 시 해당 기술이 S&T Risk Matrix 상 Red 분야인 경우 FOAB을 통해 관할 차관 또는 지정자의 사전 예외 승인 필요

2. 민감국가 정의 및 관련 조치

- (민감국가 정의) 정책적인 이유로 특별한 고려 대상이 되는 국가를 의미함. 이러한 국가는 국가안보, 핵 비확산, 지역 불안정, 국가 경제안보 위협 또는 테러 지원 등의 사유로 민감국가 목록(sensitive country list)에 포함될 수 있음
- (민감국가 목록) 현재 민감국가 목록은 외부에 공개되지 않음

〈참고〉 DOE 민감국가 관련 안내문 전문 ('25년 5월 기준)

(https : //www.energy.gov/science/what-doe-sensitive-and-other-designated-countries-list)

DOE 민감국가 및 기타 지정국가 목록이란?

- 미국 에너지부(DOE)는 내부적으로 **"민감 및 기타 지정 국가 목록"(Sensitive and Other Designated Countries List)**을 유지하고 있으며, 이는 "민감국가 목록(Sensitive Countries List)" 또는 "SCL"로 알려져 있음. 이 목록은 DOE가 직접 작성, 유지, 활용하며, 외국인과의 접촉에 관한 부처의 정책 및 절차를 지원하기 위해 운영됨.
- **SCL은 주로 다음과 같은 경우에 활용됨 :**
  1. 외국인의 DOE 시설, 정보 또는 기술에 대한 접근 시, 추가적인 DOE 내부 검토 및 승인 필요 여부를 식별하기 위해 사용
  2. 공식 해외출장의 검토 및 승인 절차에서 DOE 정책과 함께 적용
  3. 비공식 해외출장에 대한 보고 요건을 DOE 직원이 따를 수 있도록 안내
- 이 목록은 등급화된 검토 및 승인 기준을 국가별로 적용하며, **DOE 내부적으로만 사용되며, 미국 정부 외부에는 공개되지 않음**
- **SCL은 다음과 같은 행위를 금지하지 않음 :**
  1. 국제 과학기술 협력
  2. 기타 국제적 또는 학술적 교류 활동
  3. DOE 직원의 해당 국가 방문 또는 접촉
  4. 목록에 포함된 국가의 외국인이 DOE 시설을 방문하는 행위
  5. 미국 국민 또는 미국 기업의 일반적인 대외활동

– (민감국가 관련 조치) DOE 내부 규정상 민감국가 관련 조치사항은 다음과 같음

| 표 8 | DOE의 민감국가(Sensitive Countries) 관련 조치사항

주요 이슈	관련 규정	주요 조치사항
1. 국립연구소와 민감국가 간 협력 사전 검토	DOE P 485.1A	• **민감국가 국적자 또는 기관과의 협력** 시 민감국가 출신 연구자의 DOE 연구소, 연구 활동, 정보, 기술에 대한 접근 여부를 고려하여 **사전 평가 수행**
2. CRADA 체결 시 계약·재정 정보 보고	DOE O 483.1B	• DOE와 CRADA를 체결하려는 외국 기관이 **민감국가와 계약·수익(총 수입(gross income)의 10% 이상) 보유** 등 외국 이해관계 가능성이 있는 경우 **FOCI* (외국 소유·통제 영향) 심사 대상** * Foreign Ownership, Control, or Influence ※ 심사 결과에 따라 완화조치(Mitigation Measures) 요구 가능하며 여기에는 ①보안통제계획(SCP) 수립, ②기술통제계획(TCP) 수립, ③경영·의결권 등 구조 개혁, ④외국 이해관계자 배제 조치 등 포함 • **민감국가**로부터 수익이 있는 경우 **국가별 금액, 계약성격, 수출통제 준수 여부 등 상세 기재** • CRADA 체결기관이 **민감국가의 소유·지배·영향**을 받을 경우 **협력 제한 또는 해지** 가능 ※ FOCI 상태 변경 시 즉시 보고, 5년 경과 시 재평가

주요 이슈	관련 규정	주요 조치사항
3. DOE 연구소 및 기술 등 접근 제한	DOE O 142.3B	• **민감국가 국적자**의 NNSA 연구소 접근 시 **사전 신원 조사(인덱스 조회)** 필수 • 비민감 주제 접근 시에도 **인덱스 조회** 필요 (사전 완료는 불필요) ※ **인덱스 조회**는 정보·방첩국(Office of Intelligence and Counterintelligence, IN)이 주관하며, FACTS(외국인 접근 중앙추적시스템) 내 접근 요청 기록을 통해 신청 ※ 신원조사를 위해 충분한 시간이 필요하므로 **접근 시작일 최소 45일 전까지 FACTS에 입력** 권장 ※ 인덱스 조회 결과는 완료일로부터 2년간 유효하며, 만료 전에는 FACTS를 통해 자동으로 갱신 요청됨. • **민감국가 출신·소속 외국인**(언론인 포함)의 출입 시 **사전 접근 심사 및 승인 필수**이며, 해당 기록은 FACTS 시스템에 기록
4. DOE 직원의 민감국가 관련 해외출장 시 방첩 브리핑	DOE O 550.1 Chg 1, DOE O 475.1	• DOE 직원이 **민감국가 출장** 또는 **민감국가 국적자 접촉** 시 **사전 방첩 브리핑 필수**이며, 귀국 후에는 **사후 브리핑**도 IN*(정보·방첩국) 재량으로 실시 가능 * Office of Intelligence and Counterintelligence ※ 위 절차는 보안 인가(Security Clearance) 보유 여부와 무관하게 전 직원 대상 적용 • DOE 직원은 **민감국가 출신 인물과 상호작용이 포함된 해외출장**시 정보·방첩국 재량에 따라 **사전 브리핑** 및 **사후 브리핑 수행** • 민감국가 국적자의 방문 요청은 최소 30일 전에 인덱스 조회 필수
5. DOE 직원의 민감국가 비공식 여행 관련 절차	DOE O 472.2A, Chg. 1 (LtdChg)	• DOE 직원이 **민감국가로 여행**할 경우, 출발 전 현지 DOE 정보보안 담당자로부터 **사전 방첩 브리핑**을 받아야 하며, 귀국 후에는 **사후 브리핑**도 실시 가능 • 민감국가 여행 중 **경로 변경**이 발생한 경우, **귀국 후 5일 이내 보고** • 본인 혹은 직계 가족이 민감국가에 거주하게 되는 경우 3일 이내에 보고
6. DOE 방첩 프로그램 성과 평가	DOE O 475.1	• DOE의 방첩 프로그램 성과 평가 항목 중 하나로, **민감국가 외국인과의 접촉 기록의 품질, 정확성, 시의성**이 포함됨

※ 위 사항은 총괄 원칙으로, 민감국가 관련 세부 규정이나 보안관리 수준은 개별 국립연구소마다 다를 수 있음을 유의

참고 DOE 산하 국립연구소 파견 시 연구보안 유의사항 관련 파견 유경험자 인터뷰 결과

※ (참고) 연구보안 관련 상세 규정 및 보안관리 수준은 개별 국립연구소마다 다를 수 있으므로 **본 인터뷰 내용은 모든 국립연구소에 일괄 적용되는 사항은 아님을 유의**

1. 노트북에 핸드폰 연결 시 보안자료 유출 위험이 있으므로 연결 금지 또는 유의

- 보안 관리가 엄격한 연구소의 경우 노트북에 핸드폰을 연결하지 않도록 안내받았는데, 이는 핸드폰이 악성코드에 감염되었을 경우 노트북에 있는 중요한 보안 관련 정보들이 유출될 수 있기 때문임
- 특히, 충전 목적으로도 노트북에 핸드폰을 연결하지 않도록 유의해야 한다고 안내받음

2. 이메일 전송 시 기술 민감도에 따라 사전에 여러 단계의 보안 검토를 거칠 수 있음

- 민감한 기술의 경우 국립연구소뿐만 아니라 NNSA 등 상위 기관의 보안 검토를 순차적으로 거친 후에 최종 승인을 받아야 첨부파일 전송이 가능한 경우도 있음. 이 경우 이메일 전송 시 OUO(Official Use Only), CUI(Controlled Unclassified Information) 등 별도의 보안 표시를 하도록 안내받음
- 민감도가 낮은 경우 국립연구소 내부 검토만 거치거나 내부 검토 없이 이메일 전송이 가능한 경우도 있음

3. 일부 연구소에서는 출입증이나 내부 사진을 SNS 등에 업로드하는 것을 금지

- 보안 관리가 엄격한 연구소의 경우 출입증이나 내부 사진을 찍어서 SNS에 올리는 것을 금지하기도 함

4. 보안 시설의 경우 한 번에 한 명씩만 들어가도록 통제

- 모든 연구소나 시설에 해당되지는 않지만, 출입 기록을 엄격히 통제하는 곳은 한 명이 문을 잡아주고 나머지 사람들이 들어가는 것도 금지하는 경우가 있었음
- 이는 허가 받지 않은 인원의 보안시설 무단 출입에 따른 연구자산 유출을 사전에 방지하기 위한 목적임

5. 보안 업데이트를 위해 노트북을 두고 가야 하는 날이 정해져 있을 수 있음

- 연구소 내부에서만 보안 업데이트가 가능해서, 정해진 날에는 노트북을 연구소에 두고 퇴근하도록 안내받음

6. 무작위로 보안 관련 검문이 있을 수 있음

- 보안 관리가 엄격한 연구소의 경우 출퇴근 또는 업무 시 차량이나 소지품 등에 대해 불시 보안 검문을 하곤 함

7. 연구보안 관련 규정이나 요구사항 및 유의사항은 개별 국립연구소마다 다를 수 있음

- NNSA 산하 국립연구소처럼 보안관리 수준이 매우 높은 연구소는 타 국립연구소에 비해 보안관리 규정이 엄격할 수 있음
- 기초연구 위주로 수행하는 국립연구소의 경우에는 자유로운 연구 협력에 초점을 맞추는 것 같았음

3 국립과학재단(NSF)

개요

- **(개요) NSF는 외국 기관과의 협력 과정에서 발생할 수 있는 부적절한 외국 영향, 이해충돌(COI), 중복 자금 수혜(duplicate funding) 등을 방지하기 위해 연구보안 규정을 강화해 왔으며, 「CHIPS 및 과학법」에 따라 연구보안 전담 조직을 설치·운영 중에 있음**
  - 특히, 중국, 러시아, 이란, 북한 등 우려국가(Countries of Concern)와의 협력은 강화된 심사 및 검토 대상임
- **(연구보안 규정) NSF는 PAPPG* 24-1 개정('24.5.20.) 등을 통해 연구보안 관련 주요 요구사항 명시**

* NSF PAPPG(Proposal & Award Policies & Procedures Guide)는 미국 국립과학재단(NSF)의 제안 및 수상 절차에 관한 지침을 제공하는 문서임

주요 공개 및 인증 의무사항 (NSF PAPPG 24-1 기준) ('24.5.20.)

| 표 9 | 주요 공개 및 인증 의무사항

항목	기재 위치	필수 기재 내용	비고
외국 자금	Current & Pending Support	• 외국 정부, 대학, 연구소 등으로부터 수령한 연구비, 장비, 인력 등 직접·간접적 지원	SciENcv 양식 필수
외국 기관 무보수 기여	Current & Pending Support	• 외국 기관이 제공한 인력, 공간, 장비, 데이터 등 현물(in-kind) 기여 포함	무보수 공동연구 포함
외국 임용·자문·직위	Biosketch	• 외국 기관과의 임용, 자문, 겸직, 방문연구 등 모든 직위 (보수 여부 무관)	SciENcv 양식 필수
외국 협력자	COA (Collaborators & Other Affiliations)	• 공동연구자, 공동저자, 지도교수 또는 제자 관계 (최근 48개월 기준)	NSF 제공 Excel 양식 사용 필수

① 약력 스케치 : Biographical Sketch (Biosketch)

※ NSF는 외국 정부·기관과의 모든 관계(자문, 명예직, 방문연구 등)을 공개해야 하며, NSPM-33 이행 기준에 따라 보상 여부 무관하게 기재 필요

- 약력 스케치는 SciENcv 양식을 기반으로 작성하며, 학력, 직무 경력, 대표 연구업적(최대 5건), 외국 기관과의 모든 임용·직위 관계를 기재
  - 특히, 외국 기관 관련 자문, 겸직, 방문연구 등은 보수가 없더라도 모두 기재해야 하며, 이는 NSPM-33의 이행 요구사항과도 일치함

② 현재 및 보류 중인 (기타) 지원 : Current and Pending (Other) Support

- 현재 수행 중이거나 제안 중인 모든 과제는 연방·비연방 자금 여부와 관계없이 기재해야 하며, 외국 기관이 제공한 자금 외에도 장비, 인력, 공간, 데이터 등 **무보수 형태의 연구 기여 또한 포함해야 함**
- 제안서 제출 이후 관련 내용에 변경사항이 발생할 경우, **30일 이내 Research.gov를 통해 갱신해야 하며**, 기재 누락이 발견될 경우 기관 차원에서 해당 사실을 통보해야 함

③ 협력자 및 기타 제휴 : Collaborators & Other Affiliations (COA)

- 공동연구자, 공동저자, 학위 지도교수 또는 제자 등과의 관계는 과거 4년간의 이력을 기준으로 모두 기재해야 하며, 이 정보는 NSF의 심사위원(Peer Reviewer) 배정 시 이해충돌(COI) 여부 판단에 활용됨
- SciENcv 양식이 아닌 별도의 Excel 템플릿을 사용해야 하며, 서식 누락은 규정 위반으로 간주됨

악성외국인재유치프로그램 금지 : Prohibition on Malign Foreign Talent Recruitment Programs (MFTRP)

2024년 5월 20일 이후 제출되는 제안서부터, 모든 Senior/Key Personnel은 자신이 현재 또는 과거 MFTRP에 참여하지 않았음을 개별적으로 인증(Certification) 해야 함

- 해당 인증은 기관 차원의 인증과는 별도로 각 개인이 직접 수행해야 함

MFTRP는 주로 우려국가(Foreign Countries of Concern) 및 관련 기관에서 운영하는 프로그램으로, 다음과 같은 조건 중 하나 이상에 해당할 경우 MFTRP 참여로 간주

- 미공개 기술·자료·성과의 외국 이전 요구, 외국 기관의 기금 수령 강제, 이중 소속 또는 겸직 강요, 미국 소속기관 표시 제한, 참여 계약의 종료 제한

MFTRP 참여자는 NSF 수혜 대상에서 제외되며, 허위 기재 또는 미공개 시 NSF OIG 조사 및 연방 기금 수혜 제한 등 제재 가능

(기관 요건) 연구보안계획 자체 인증 : Certification of Research Security Plan

NSF로부터 총 50만 달러($500,000) 이상을 수혜받는 기관은 다음 항목을 포함하는 연구보안계획을 자체적으로 인증(Certify) 해야 함

- 공식 연구보안 프로그램(Research Security Program)
- 연구의 책임 있는 수행(RCR, Responsible Conduct of Research) 교육 제공
- 사이버보안, 외국 영향, 데이터 관리 정책 포함

본 인증은 NSF에 의해 별도 심사되지는 않지만, 정직하고 완전한 제출이 전제되며, 허위로 인증할 경우 연방 차원의 제재 대상이 될 수 있음

연구보안 규정 위반 시 조치 (NSF PAPPG 기준)

| 표 10 | 위반 시 조치

위반 유형	예시	조치
누락 기재	외국 자금, 무보수 협력 등 미기재	제안서 반려, 협력 철회
허위 기재	외국 자금 은폐, 관계 은폐	수상 취소, 향후 자격 제한, NSF OIG 조사
MFTRP 관련 불성실 신고	과거 참여 이력 은폐	NSF OIG 조사 및 연방 기금 수혜 제한 등 제재 대상이 될 수 있음

Tip! NSF 사업에 참여하고자 하는 연구자를 위한 상세 유의사항

〈 NSF 연구보안 규정 관련, 국제공동연구시 유의사항 〉

1. 외국 협력의 공개 범위가 큰 폭으로 확장된 것에 유의

- NSF는 외국 기관으로부터의 모든 지원, 자문, 협력관계를 보수 여부와 관계없이 공개할 것을 요구하고 있음
- 예를 들어, 우리나라 연구자가 미국 연구자와 공동연구를 수행하는 경우, 다음과 같은 사례도 모두 공개 대상에 해당됨 :
  - 우리나라 연구기관이 외국으로부터 연구공간, 인력, 장비, 데이터를 제공받은 경우
  - 미국 연구자와 공동 논문 또는 공동 프로젝트 수행 중인 경우
  - 미국 측 연구책임자(PI)가 우리나라 기관의 방문연구원으로 활동 중일 경우

☑ Tip | 미국 연구자의 제안서에 본인의 이름, 소속, 역할이 포함될 수 있으므로, 자신의 기관 정보, 역할, 기여 내용 등을 사전에 정리하여 제공하고, 해당 내용이 NSF 제출 문서에 어떻게 기재되는지 사전 확인 필요

2. 무보수 활동도 Disclosure 대상임

- NSF는 "보수를 받지 않더라도 실질적 연구 기여가 있는 관계"는 Current & Pending Support 문서에 포함해야 한다고 명시
- 예를 들어, 우리나라 연구자가 미국 측 연구에 단순 조언을 하거나 공동 실험을 제공한 경우, 보수를 받지 않았더라도 NSF 측에서는 자원 제공 또는 연구 지원으로 간주할 수 있음

☑ Tip | 무보수라 하더라도 실질적 연구 기여가 있는 경우에는 Disclosure 대상일 수 있으므로, 기여 내용과 범위를 명확히 정리해 미국 측 PI에 전달

3. 협력기관이 아닌 경우에도 규정이 간접 적용될 가능성에 유의

- 우리나라 기관이 NSF 과제의 하위 수혜기관(subrecipient) 또는 공동연구 참여기관으로 명시되지 않더라도 미국 측 기관이 총 50만 달러($500,000) 이상의 연구비를 수혜받는 경우, 기관 차원의 연구보안 프로그램 인증서 제출이 필요할 수 있음
- 미국 측 기관은 협력기관에 보안관리, 연구윤리 교육, 외국 영향 통제 절차의 이행을 요구할 수 있음

☑ Tip | 본인 소속 기관이 NSF와 직접 계약하지 않더라도, 미국 측 기관으로부터 보안 관련 요구사항(서약서 제출, 교육 이수, 연구자산 관리 등)을 요청받을 수 있음을 사전에 인지하고 이에 대한 대응 체계 마련 필요

4. MFTRP(Malign Foreign Talent Recruitment Program) 관련 각별한 주의 필요

- NSF는 모든 연구책임자(PI) 및 Senior Personnel에게 자신이 악성 외국 인재 유치 프로그램(MFTRP)에 참여하고 있지 않음을 증명할 것을 요구하고 있음
- 해당 요건은 NSF 제안서 제출 시점뿐 아니라, 과제 수상 이후에도 매년 재확인 절차가 요구됨

☑ Tip | 과거 해외 정부 또는 대학으로부터 연구비, 명예직, 자문 역할을 부여받은 이력이 있는 경우, 해당 관계가 MFTRP로 간주될 가능성이 있는지 면밀히 검토하고, 필요 시 미국 측 PI와 함께 설명자료를 사전에 준비해 둘 필요가 있음

그래도 궁금해요! NSF 사업에 참여하고자 하는 연구자를 위한 FAQ

| 표 11 | NSF 연구보안 규정 관련 FAQ

질문	설명	대응방안
외국 기관으로부터 무보수로 지원받은 공간이나 인력도 공개해야 하나요?	무보수라도 외국 기관으로부터 연구자원(공간, 장비, 인력 등)을 제공받았으면 공개 대상임	외국 기관으로부터 지원받은 내용이 있는 경우 관련 정보를 투명하게 공개
외국 연구자와 공동 저자로 논문을 썼다면 Disclosure 해야 하나요?	4년 이내 공동저자인 경우 COA 양식에 포함될 수 있음	공동저자 관계가 있다면 미국 측에 알려 COA 양식에 포함될 수 있도록 할 필요
우리나라 연구자도 MFTRP 참여 여부를 확인해야 하나요?	NSF 제안서에 포함된 모든 Senior Personnel은 MFTRP 참여 여부를 확인해야 함	과거 MFTRP 참여 여부를 확인하고, 투명하게 공개 필요
우리나라 기관은 $500,000 이상 프로젝트에도 보안계획을 제출해야 하나요?	우리나라 기관은 직접 수혜기관은 아니더라도 Subaward로 참여 시 요구받을 수 있음	보안계획이 요구되는 경우 미국 측과 사전 협의해 템플릿을 공유받아 대응 필요
Disclosure 정보 누락 시 어떤 문제가 생기나요?	정보 누락은 NSF 수상 취소, 감사, 수사, 향후 제안 제한 등의 결과를 초래할 수 있음	정보 제출 전 NSF PI와 교차 검토하고, 논란의 여지가 있는 부분은 사전 설명서를 첨부

4 국립보건원(NIH)

개요

(개요) 국립보건원(NIH)은 미국 내 생물의학 연구의 무결성 보호를 위해, 연구자 및 기관이 외국 활동을 포함한 모든 연구 자원, 과학적 협력, 그리고 재정적 이해관계를 투명하게 공개할 것을 요구

- 과학적, 예산적, 업무적 중복(overlap)을 방지하고, 국제 협력 속에서도 미국 연구 시스템의 신뢰성을 유지하기 위한 목적임

(연구보안 규정) 재정적 이해 상충 및 외국 구성 요소 관련 기타 지원에 대한 NIH 정책 알림*을 통해 기존 정책을 재강조

* Reminders of NIH Policies on Other Support and on Policies related to Financial Conflicts of Interest and Foreign Components [NOT-OD-19-114 (2019.7.10.)]

※ 2018년 NIH는 생의학 연구의 무결성을 보호하기 위한 검토를 시작했고, 국제 협력은 장려하되 투명성과 충돌 방지가 핵심임을 강조함. 해당 공지는 기존 정책의 재강조이며, 새로운 정책 변경이 아님

주요 공개 항목 및 의무 사항

① 기타 지원 (Other Support)

- 정의 : 연구자가 수행하는 모든 연구 활동에 관련된 자금, 자원, 인력 지원 등 (금전 여부 불문)
- 보고 대상 :
  - 외국 및 국내 기관으로부터의 연구비, 실험실 인력 지원
  - 고가 장비, 공간, 생물자원, 실험 재료 등 현물(in-kind) 자원
  - 외국 인재 유치 프로그램(Foreign Talent Recruitment Program) 참여
- 요구사항 :
  - Senior/Key Personnel의 모든 활동에 대해 인력 기여(person-months), 총 지원 금액, 자원 출처 등을 포함
  - 제안서 제출 전에는 Just-in-Time(JIT) 단계에서 보고
  - 수상 이후 변경사항 발생 시에는 연례 RPPR 보고서 제출 또는 NIH에 사전 승인 요청

    ※ (예) 한국 기관이 미국 PI에게 실험 인력과 실험 공간을 제공할 경우 → NIH에는 Other Support로 보고 필요

② 외국 구성요소 (Foreign Components)

- 정의 : NIH 지원 연구의 일부 또는 전체가 미국 외부에서 수행되는 중요한 과학적 요소 또는 세그먼트를 의미하며, 다음 중 하나 이상에 해당할 경우 Foreign Component로 간주됨
  - 연구자 또는 수혜자가 미국 외부에서 연구 활동을 수행하는 경우
  - 외국 기관에 고용되었거나 외국 기관으로부터 급여를 받는 연구자가 외국에서 연구를 수행하는 경우
- 보고 필요 시점 :
  - 최초 제안서 제출 시 또는 과제 수행 도중 Foreign Component가 추가되는 경우에는 반드시 NIH의 사전 승인 필요 (NIHGPS §8.1.2)

    ※ (예) 미국 PI의 NIH 과제에서 한국 연구자가 일부 실험을 한국에서 수행할 경우 → Foreign Component로 간주되어 사전 승인 필요하며, 단순한 공동저자 관계나 협의성 출장 등은 Foreign Component로 간주되지 않음

③ 재정적 이해충돌 (FCOI, Financial Conflict of Interest)

- 법적 근거 : 42 CFR Part 50, Subpart F (연구의 객관성에 관한 규정)
- 보고 대상 : 외국 기관에서 발생한 중대한 재정적 이익(Significant Financial Interest)
- 보고 방식 : 연구자가 소속 기관에 FCOI를 공개하고, 기관은 자체 기준에 따라 NIH에 보고

  ※ 연구자가 NIH에 직접 보고하는 것이 아니라, 우리나라 연구기관이 NIH에 보고하는 형식임을 유의
- 기타 사항 :
  - FCOI는 Other Support 및 Foreign Component와는 별개의 독립된 보고 체계임
  - 기관의 자체 정책이 NIH 기준보다 엄격한 경우, 해당 기관 기준을 우선 적용

| 표 12 | NIH에 보고가 필요한 사례 예시

사례	기타 지원 (Other Support)	외국 구성요소 (Foreign Compoments)	재정적 이해충돌 (FCOI)
한국 기관에서 장비 제공	○	X	X
한국 연구자가 실험 수행	○	○	X
외국 기업 지분 보유	X	X	○
외국 기관 자문직 (무보수)	○	X	조건에 따라 필요*

* 자문 활동이 향후 금전적 이익을 수반하거나, 판단 기준을 초과하는 경우에는 FCOI로 간주될 수 있음.

보고 시점 및 방식

- 기타 지원(Other Support) :
  - 제안서 제출 직전 : Just-in-Time(JIT) 단계에서 제출
  - 수상 후 변경 발생 시 : RPPR 또는 사전 승인 요청 필요
- 외국 구성요소(Foreign Component) :
  - 제안서 제출 시 또는 연구 도중 추가되는 경우 NIH의 사전 승인 필수
- 재정적 이해충돌(FCOI) :
  - 기관 기준에 따라 연 1회 이상 평가하며, NIH에 보고 의무 발생 시 통지

Tip! NIH 사업에 참여하고자 하는 연구자를 위한 상세 유의사항

〈 NIH 연구보안 규정 관련, 국제공동연구 시 유의사항 〉

1. 외국으로부터 제공받는 자원은 NIH에 공개 대상임을 인지할 필요

- NIH는 연구자가 수행하는 모든 연구활동에 대해, 금전적 가치와 무관하게 제공된 모든 자원을 Other Support(기타 지원) 항목에서 투명하게 공개할 것을 요구하고 있음
- 외국 기관이 제공한 실험 공간, 고가의 실험 장비, 인력(예 : 기술 인력, 박사후연구원 등), 실험 물질 등도 모두 포함

☑ Tip | 우리나라 기관이 NIH 과제와 관련된 공동연구에서 외국으로부터 자원을 제공받고 있다면 NIH에 Other Support로 보고해야 하므로, 사전에 제공 내역을 문서화하고 공유

2. 실험이 우리나라에서 수행된다면 Foreign Component로 보고 대상에 해당할 수 있음

- NIH는 연구의 일부가 미국 외 지역(예 : 우리나라 등)에서 수행되는 경우를 Foreign Component(외국 구성요소)로 간주하며, 이에 대해 사전 승인을 받도록 규정하고 있음
- 특히, NIH 자금이 사용되지 않더라도, 우리나라 연구자가 실질적인 실험 수행을 한다면 Foreign Component로 간주

☑ Tip | 공동 실험이 우리나라에서 수행되는 경우, 수혜기관이 이를 Foreign Component로 판단하고 NIH에 사전 승인 요청을 해야 하므로, 해당 연구활동의 내용과 역할을 명확히 설명하고 사전에 협의할 필요

3. 외국 기관과 관련된 임용·자문·인재 프로그램 참여는 반드시 공개 대상임을 유의

- 연구자가 외국 기관에서 직위(정규직, 자문, 명예직 포함)를 보유하거나 인재 프로그램(예 : 해외 과학자 유치 사업)에 참여하고 있는 경우, 해당 내역은 NIH의 Other Support 문서 또는 Biosketch에 공개해야 함
- 보수를 받지 않는 경우라도, 해당 활동이 연구와 관련된 경우에는 모두 공개 대상임을 유의해야 함

☑ Tip | 우리나라 연구자가 NIH 과제에 Senior/Key Personnel로 포함될 경우, 외국 관련 모든 관련 직위 및 프로그램 참여 내역을 사전에 정리하고 공개 대상 여부를 사전 확인

4. 재정적 이해충돌(FCOI)은 기관을 통해 보고해야 하며, 외국 재정도 포함됨

- NIH는 별도의 규정(42 CFR Part 50, Subpart F)에 따라, 연구자가 보유한 외국 기업·기관으로부터의 재정적 이익도 소속 기관을 통해 보고하도록 요구하고 있음
- 해당 보고는 Other Support와는 별도로 관리되며, 소속 기관의 자체 기준이 NIH보다 더 엄격할 경우 소속 기관 기준을 준용

☑ Tip | NIH 과제 수행 중 외국 자금, 주식, 지분 보유, 기업 계약 등이 발생할 가능성이 있다면, 소속 기관의 FCOI 기준을 검토하고, 필요시 기관을 통해 사전 보고 절차를 이행해야 함

5. NIH에 공개해야 하는 정보는 수상 전·후 모두 반영되어야 하며, 변경 시에는 즉시 NIH에 통지 필요

- Other Support는 NIH 제안 제출 시점뿐만 아니라, 수상 직전(JIT), 수상 후 연례보고(RPPR), 그리고 변경사항 발생 시에도 모두 반영되어야 함

☑ Tip | 공동연구 진행 중 외국 기관으로부터 새로운 지원이 추가될 경우, NIH에 통지 필요

그래도 궁금해요! NIH 사업에 참여하고자 하는 연구자를 위한 FAQ

| 표 13 | NIH 연구보안 규정 관련 FAQ

질문	설명	대응방안
우리나라 연구자의 외국 기관 겸직이나 자문 활동도 공개해야 하나요?	무보수라도 외국 임용·자문 등은 공개 대상임	외국 기관과의 관계가 있다면 해당 사항을 NIH에 투명하게 공개 필요
우리나라 연구자가 NIH 자금을 직접 받지 않아도 정보 공개 대상인가요?	간접 참여라도 Senior/Key Personnel으로 지정되면 정보 공개 대상	Senior/Key Personnel로 지정되었는지 확인하고 정보 공개 범위 내역을 정리
공동연구 중 새롭게 지원이 추가되면 해당 정보를 수정해야 하나요?	수상 전후에도 계속 갱신되어야 하며 변경 시 즉시 통지할 필요	연구 중 자원 추가 시 즉시 미국 측에 알리고 관련 정보 갱신 요청
정보 누락 시 불이익이 있나요?	연구비 환수, 지원 중단, 법적 제재 등으로 이어질 수 있음	문서 제출 전후로 내용을 교차 검토하고, 의심 소지가 있는 경우에는 사전 설명자료를 마련해 대응 필요
FCOI는 Other Support와 어떤 점이 다른가요?	FCOI는 외국 재정 이해관계 공개 의무로, 연구자가 아닌 연구기관이 NIH에 별도로 보고해야 함	FCOI는 기관 기준에 따라 별도 보고되므로 기관 정책도 함께 검토

5 항공우주국(NASA)

개요

(개요) NASA의 Grant and Cooperative Agreement Manual (GCAM)은 보조금 및 협력 협정과 관련된 정책 지침을 제공하며, 연구보안, 수출통제, 외국 참여자 관리 등 기술 보호와 관련 주요 조항을 명시하고 있음

NASA의 연구보안 및 기술 보호 관련 조항

※ GCAM(Grant and Cooperative Agreement Manual, 2025년 3월판)에 명시

① 수출통제 (Export Control)

※ GCAM §16.7–§16.9

- (16.7 Export Control) 외국 기관 또는 외국 국적자의 참여가 포함된 경우, 미국의 수출통제법(ITAR, EAR 등) 적용 가능성을 사전에 고려해야 하며, 수혜 기관은 관련 법규 준수에 전적인 책임을 져야 함
- (16.8 Export-Control Guidelines for Foreign Participation) 제안서에 외국 참여가 포함되는 경우, 해당 활동이 수출통제 대상에 해당하는지를 사전에 평가해야 하며, 필요시 다음 사항을 포함해야 함 :
  - 기술지원협정(TAA) 또는 수출허가 보유 여부
  - 기술이전통제계획(TTCP, Technology Transfer Control Plan)
- (16.9 Export-Controlled Material in Proposals) 수출통제 대상 기술자료는 제안서에 포함하지 않을 것을 강력히 권장하나, 제안서에 포함될 경우에는 다음 요건을 반드시 준수해야 함 :

  ※ NASA는 미국 시민권 또는 영주권을 보유하지 않은 외국인을 심사위원으로 위촉할 수도 있으므로, 해당 자료의 포함 여부에 대해 사전 신중한 검토 필요
  - 문서 상단에 수출통제 고지문(예 : “This document contains export-controlled information subject to [법령명]”)를 삽입
  - 관련 내용은 별도 구분 및 식별 처리

② 보안 및 연구 부정행위(Security & Research Misconduct)

※ GCAM §16.12, §16.15

- (16.12 Security) 보안 요건이 수반되는 경우 NASA의 보안정책 및 법령을 준수해야 하며, 외국인의 접근은 제한될 수 있음
- (16.15 Research Misconduct) 14 CFR Part 1275에 따라 위조, 변조, 표절 등은 ‘연구 부정행위’로 간주되며, NASA OIG(감찰실)의 조사 대상이 될 수 있음

③ 악성외국인재유치프로그램 (Malign Foreign Talent Recruitment Programs (MFTRP))

※ GCAM §16.16

- 「CHIPS and Science Act of 2022」 §10631에 따라, MFTRP 참여자는 NASA 보조금 수혜 대상에서 원칙적으로 제외됨

- 적용 대상 :
  - PI(연구책임자), Co-PI(공동연구책임자)
  - 연간 참여율 10% 이상인 Co-Investigator(Co-I, 참여연구원)
- 모든 해당 인력은 제안서 제출 시 및 매년 MFTRP에 해당되지 않음을 자가 인증해야 하며, 수혜기관은 관련 문서 보관 의무가 있음

④ 외국 참여 명시 요건

※ GCAM §10.8.4, §10.11

- (10.8.4 Foreign Proposals) 외국인·외국 기관 참여 시, 소속, 역할, 자금흐름, 기술 접근범위 등을 상세히 명시하고 관련 서류(LOI 등) 첨부 필수
- (10.11 Data Management Plan(DMP)) 데이터 접근권, 보존방식, 외국인 접근 여부 등을 계획서에 기술해야 하며, 제한 기술인 경우 별도의 보호 계획 요구됨

NASA의 Foreign Participation (외국 참여자) 관련 정책

※ NASA FAR Supplement(2025년 1월판)에 명시

① 정의 및 범위

- 외국 참여자(Foreign Participants)는 다음을 포함하며, 우리나라 국적자 및 기관 모두 포함됨 :
  - 미국 외 지역에 설립된 기관 (대학, 연구소, 기업)
  - 미국 내에 소재하나 외국 소유 또는 통제 기관
  - 외국 국적자

    ※ 정의는 NASA FAR Supplement(NFS) §1835.016-70, §1852.235-72, §1852.225-70 및 NPR 1600.4A 등에서 명시됨

② 사전 검토 및 제한 원칙

- NASA Guidebook for Proposers에 따라 외국 참여자는 다음 사항을 사전에 공개해야 함 :
  - 소속 및 역할, NASA 펀딩 지원 여부 및 해당 예산 항목, 특정 외국 정부와의 연계 또는 협력 여부 등
- 정보 누락 시 NASA는 제안서 자체를 심사에서 제외하거나 수상 후 제한 조치를 취할 수 있음

③ NASA FAR Supplement (NFS) 관련 조항

- NASA 계약/협약의 기준이 되는 NASA FAR Supplement (NFS)는 외국 참여자와 관련하여 다음 항목을 명시 :
  - (NFS 1835.016-70) 외국 참여자 참여 시 NASA 계약관리자의 사전 승인 필요
  - (NFS 1852.235-72) 외국 참여자의 역할과 접근 권한을 명시하는 계약 조항 삽입
  - (NFS 1852.225-70) Foreign Nationals employed by NASA Contractors – 외국인 고용 시 보고 및 승인 의무

Tip! NASA 사업에 참여하고자 하는 연구자를 위한 상세 유의사항

〈 NASA GCAM 연구보안 규정 관련, 국제공동연구 시 유의사항 〉

1. 외국 참여자로서의 법적 지위를 인식하고 투명한 정보 공개 필요

- NASA는 미국 외의 국적을 가진 연구자 및 기관을 Foreign Participant로 간주하므로 우리나라 국적 연구자나 기관은 NASA와 협업 시, 자신이 외국 참여자임을 전제로 하고, GCAM 10.8.4 및 16.8에 따라 역할, 책임, 기술 접근 범위, 특정 외국 정부와의 관계(소유·자금 지원) 등을 사전에 명시해야 함

☑ Tip | 자신의 신분, 소속 기관, 연구 기여 내용 등을 명확히 문서화하고 제안서에 반영되도록 협의

2. 수출통제(Export Control) 대상 기술 포함 여부를 사전 검토

- GCAM 16.7~16.9에 따르면, NASA와의 협력 연구 중 ITAR(무기 수출통제법) 또는 EAR(상무부 수출관리규정)의 적용을 받는 기술이 포함될 경우, 외국 참여자는 해당 기술에 자유롭게 접근할 수 없음

☑ Tip | 필요시 연구참여 내용이 수출통제 대상에 해당될 가능성이 있는지 협의 후 관련 통제계획 수립 협력

3. 악성 외국 인재 프로그램(MFTRP) 참여 경력이 있다면 NASA와의 협력에 제한될 수 있음

- GCAM 16.16에 따르면, Malign Foreign Talent Recruitment Program(MFTRP) 참여 이력이 있는 경우, NASA 지원 과제에 참여할 수 없거나, 심사·수상에 제한을 받을 수 있음

☑ Tip | 과거 악성 외국 인재 프로그램 참여 이력이 있다면, 해당 정보를 공개하고 필요시 관련 사유 등을 해명

그래도 궁금해요! NASA 사업에 참여하고자 하는 연구자를 위한 FAQ

| 표 14 | NASA GCAM 연구보안 규정 관련 FAQ

질문	설명	대응방안
우리나라 연구자가 NASA의 보안시설에 접근할 수 있나요?	시스템 접근이 제한되거나 사전 보안 심사가 필요할 수 있음	접근 권한을 사전에 확인하고 NDA 또는 접근 제한 문서에 서명
과거 외국 인재 유치 프로그램(MFTRP)에 참여한 경력이 있으면 NASA 과제 참여에 제한이 있나요?	NASA GCAM은 MFTRP 참여자에 대한 협력 제한을 명시	참여 이력이 있다면 관련 내용을 투명하게 공개하고, 필요시 세부 내용에 대해 해명
연구 결과물이 한국 측 연구자에게도 귀속되나요?	공동 개발 기술은 NASA 조건에 따라 NASA 또는 공동기관에 귀속될 수 있음	계약서 또는 협약서에 기술 귀속 및 사용권 조항을 명확히 포함
제안서에 외국 참여자 정보를 명시하지 않으면 어떻게 되나요?	미기재 시 제안서 평가 제외 또는 협력 제한 조치가 이루어질 수 있음	외국 참여자 항목은 제안서 내 필수 항목이므로 누락 없이 기재
연구 보안 위반 시 어떤 제재를 받을 수 있나요?	NASA OIG의 감사 대상이 될 수 있으며, 수혜 제한, 계약 해지 등이 발생할 수 있음	연구보안 교육 이수 및 모든 관련 정보 사전 공유·문서화 체계를 갖출 것

6 국방부(DoD)

개요

- (개요) 국방부(DoD)는 국방과학기술 연구에 대한 외국의 부적절한 개입을 방지하고, 연구의 무결성과 국가안보를 보호하기 위해 외국 인재 프로그램 대응, 민감정보 보호, 핵심 인력 보호, 기술유출 방지를 포함한 연구보안 정책을 운영
  - 2019년 「국방수권법(National Defense Authorization Act for Fiscal Year 2019, NDAA FY2019)」 제1286조(Protection of National Security Academic Researchers)는 국방장관에게 연구보안 강화를 위한 제도적 조치를 마련할 법적 권한과 의무를 부여
  - 이에 따라 DoD는 2019년 3월 20일, 「연구보호 조치 관련 메모(Actions for the Protection of Intellectual Property, Controlled Information, Key Personnel and Critical Technologies)」를 발행하여 외국 참여자에 대한 공개(disclosure) 요건을 포함한 구체적인 이행 지침을 발표

외국 자금·활동·관계에 대한 정보 공개 의무

- DoD는 2019년 3월 20일 메모(March 20, 2019 Memo)를 통해, DoD가 발행하는 모든 새로운 연구지원 공고(Notice of Funding Opportunity, NFO)에 다음과 같은 'Current and Pending Support(현행 및 예정된 지원)' 정보 제출 의무를 포함
  - 연구자가 현재 수행 중이거나 신청 중인 모든 과제 내역
  - 각 과제의 제목 및 목표
  - 각 과제에 연구자가 연간 투입하는 비율(시간 기준)
  - 각 과제의 전체 지원 금액
  - 지원 기관의 명칭 및 주소
  - 과제의 수행 기간
- 이 정보는 해당 연구 과제에서 핵심 인력(Key Personnel)으로 지정된 모든 인물에 대해 제출해야 하며, 이를 제출하지 않을 경우 제안서 평가에서 제외될 수 있음을 명시

악성 외국 인재 유치 프로그램(MFTRP) 금지 조항

- NDAA FY2019 제1286조는 미국 국방장관에게 다음과 같은 정책을 수립·시행할 것을 요구
  - 국가안보와 관련된 학술 연구자의 보호(Protection of National Security Academic Researchers)를 위한 제도화
  - 외국 인재 유치 프로그램(Foreign Talent Programs) 등 외국 정부 주도의 불법적 기술 유출 시도에 대한 제재 조치 마련
  - 방위기술 연구를 수행하는 미국 내 기관의 지식재산(IP), 통제정보(CUI), 핵심 인력, 민감 기술 보호 시스템 확립

» 특히, 2024년 8월 9일 이후부터는, MFTRP 참여 인력이 포함된 과제, 또는 MFTRP 관련 내부 정책을 보유하지 않은 기관은 DoD로부터 기초연구 자금을 수혜받을 수 없음

※ (근거) 「Countering Unwanted Foreign Influence in Department-Funded Research」

- 각 참여기관은 연 1회 RPPR(Research Performance Progress Report)를 통해 참여자 전원의 MFTRP 관련 참여 여부를 확인해야 함
- 보안심사로 인해 제안서가 반려되는 경우, DoD는 사유를 서면으로 통보하며, 제안기관은 DoD의 연구·엔지니어링 차관실(OUSD(R&E))에 이의제기를 요청할 수 있음. 해당 사안은 중앙조정기구가 검토 후 결정 변경 여부 판단

외국 영향 평가를 위한 보안심사 및 참여 제한

» DoD는 2023년 6월 「Countering Unwanted Foreign Influence in Department-Funded Research」를 통해 모든 기초연구(fundamental research) 과제 제안서에 대한 보안심사(Security Review)를 도입하였는데, 이는 기술적 평가와 별도로 다음과 같은 외국 영향 요소에 대한 위험기반 심사(Risk-Based Security Review)를 진행하는 절차임

- DoD는 “의사결정 매트릭스(Decision Matrix)”를 통해 외국 영향 관련 행동을 4가지 주요 요소로 평가하며, 보안심사 항목에는 다음과 같은 4가지 외국 관련 지표가 포함됨 :
  - 외국 인재 유치 프로그램(FTRP, MFTRP) 참여
  - 우려국가(FCOC) 또는 그 기관으로부터의 자금 수령
  - 특허 출원/보유 내역 (특히 미국보다 외국 선출원 여부)
  - 미국 상무부 BIS(Entity List 등)에 등재된 기관과의 연관성
- 보안심사 결과는 다음 4단계 조치로 구분됨 :
  - 금지(Prohibited) : MFTRP 참여자 등은 원천적 수혜 금지
  - 제한 또는 완화(Mitigation required) : 위험 요소 있음 → 보완조치 조건부 수혜 가능
  - 정보제공 필요(Disclosure only) : 정보 제출 의무
  - 무조치(No action) : 위험 없음

Tip! DoD 사업에 참여하고자 하는 연구자를 위한 상세 유의사항

〈 DoD 연구보안 규정 관련, 국제공동연구시 유의사항 〉

1. 악성 외국 인재 프로그램(MFTRP) 참여 이력이 있다면 DoD 협력에 제약을 받을 수 있음

- DoD는 악성 외국 인재 유치 프로그램(Malign Foreign Talent Recruitment Programs, MFTRPs) 참여자를 연구 협력에서 제한하거나 배제할 수 있음

☑ Tip | 과거 외국 인재 프로그램 참여 이력이 있다면, 참여 시기, 내용, 현재 종료 여부 등을 명확히 정리하고, 필요 시 해명문서 또는 서면 설명을 미국 측에 제공할 준비를 해야 함

3. 연구자가 받은 모든 외국 자원, 소속, 지원을 투명하게 공개할 필요

- DoD는 자금의 출처, 인적 자원의 제공, 외국 기관 겸직, 명예직, 공동저자 활동 등까지 공개 범위에 포함시킴
- 금전적 가치가 없어도, 연구 수행과 관련된 자원은 모두 공개 대상임

☑ Tip | 우리나라 연구자가 외국으로부터 인건비, 공간, 실험장비 등의 자원이 있을 경우 해당 사항을 투명하게 공개

그래도 궁금해요! DoD 사업에 참여하고자 하는 연구자를 위한 FAQ

| 표 15 | DoD 연구보안 규정 관련 FAQ

질문	설명	대응 방안
과거 외국 인재 유치 프로그램(MFTRP) 참여 이력이 있으면 제한되나요?	과거 MFTRP 참여자는 정보 공개 또는 협력 제한 대상이 될 수 있음	참여 사실과 내용을 정리하여 투명하게 공개하고 필요시 사전 설명을 준비
국외 수혜 관련, 어떤 정보까지 포함되어야 하나요?	외국 기관 소속, 자금, 직위, 자원, 명예직 등 모든 외국 관련 사항을 포함	국외 수혜 항목을 정기적으로 갱신

제4장

미국과 국제공동연구시 연구보안 가상 사례

제4장. 미국과 국제공동연구시 연구보안 가상 사례

※ 본 사례는 실제 공개된 규정, 정책, 보도자료, 인터뷰 등을 바탕으로 정책적 이해를 돕기 위해 창작한 가상의 시나리오이며, 특정 기관, 인물 또는 실제 사건과는 무관함

가상사례 ❶ 정보 접근 통제의 중요성 : 접근권한 관리 이슈

개요

- C연구원은 한국의 D연구소 소속으로, 미국 국립연구소와 CRADA 체결을 통해 공동으로 특정 에너지 재료의 설계 및 해석 관련 기술을 연구 중임. 해당 연구는 민감 기술 정보를 포함하고 있었으며, 미국 측은 이 중 일부를 Controlled Unclassified Information (CUI)로 지정하여 관리
- 초기에는 C연구원의 시스템 접근 권한이 제한적으로 설정되어 있었으나, 연구 진행 중 권한 설정 과정에서 클라우드 기반 폴더에 대한 접근 가능성이 발생
- C연구원은 사전 정보 없이 해당 폴더를 열람하고 일부 자료를 내려받았으며, 이후 정기적인 시스템 감사 과정에서 이 기록이 식별됨

※ (참고) 본 사례는 현행 규정 등을 바탕으로 창작한 가상의 시나리오이며, 특정 기관이나 실제 사건과는 무관

적용 가능 규정 예시

규정/지침	주요 내용
DOE O 142.3B	외국인의 DOE 관련 시스템·시설 접근은 사전 승인을 포함한 절차에 따라야 함
DOE P 485.1A	외국 연구자와의 협력 시 민감 기술의 범위와 접근 조건을 명확히 설정해야 함
DOE O 471.1 (CUI)	CUI는 사전에 승인된 경로를 통해서만 접근 가능하며, 지정된 통제체계를 통해 보호되어야 함

연구보안 이슈

» 외국 연구자의 CUI 접근은 DOE의 보안 절차, 신원확인, 정보보호 교육 이수 여부 등 사전 요건에 기반하여 엄격히 관리되므로 해당 규정을 준수 필요

연구자 유의사항

- 우리나라를 포함한 외국인 연구자는 CUI에 자동적으로 접근 권한이 부여되지 않으며, 미국 측 협력기관이 설정한 범위 내에서 승인된 정보에만 접근해야 함
- DOE 산하 과제에 참여하거나 CRADA 등을 통해 공동연구를 수행하는 우리나라 연구자는 사전에 DOE 또는 미국 국립연구소 측에서 요청하는 보안 교육을 성실히 이수하고, 본인의 접근 권한 범위와 제한 조건을 인지

가상사례 ② 기술 특성에 따른 접근 제한… 사전 인지가 필요

개요

- H연구원은 한국의 A소재과학연구소 소속으로, 미국 에너지부(DOE) 산하 국립연구소와 공동으로 특정 소재 개발 과제에 참여 중임. 해당 과제는 DOE의 연구개발 프로그램 하에 수행되었으며, 미국 측 연구기관은 관련 기술을 Science & Technology (S&T) Risk Matrix에서 Yellow 등급으로 분류하고 있음
- Yellow 등급 기술은 기술적 복잡성과 응용 가능성에 따라 일정 수준의 안보 고려가 필요한 분야로, 외국 국적 참여자의 기술 접근에는 추가적인 검토 및 통제 절차가 적용될 수 있음
- 과제 초기에는 H연구원이 협력 범위 내에서 참여했으나, 기술 범위가 확대되며 기술 민감도 재평가가 이루어졌고, 이에 따라 일부 실험 설계 및 분석 작업에 대한 참여 조정이 이루어짐

※ (참고) 본 사례는 현행 규정 등을 바탕으로 창작한 가상의 시나리오이며, 특정 기관이나 실제 사건과는 무관

적용 가능 규정 예시

규정/지침	주요 내용
DOE Science & Technology Risk Matrix	기술 민감도에 따라 Red, Yellow, Green 등급으로 구분. Yellow는 특정 조건에서 외국인 접근 시 사전 검토 및 보안조치 필요
DOE O 142.3B	외국인 연구자의 DOE 시설·정보·기술 접근은 사전 심사 및 승인 대상임

연구보안 이슈

» S&T Risk Matrix 상 Yellow 등급 기술은 기본적으로 협력 가능성을 열어두고 있으나, 해당 기술의 민감도와 국가안보 관련성 평가에 따라 외국인의 기술 접근은 사전 검토와 기관 간 협의에 따라 조정될 수 있음

» 이러한 기술은 일반적으로 선별적 정보 접근, 역할 조정, 보안계획 수립 등을 통해 협력이 추진되며, 이는 연구보안 정책의 일환임

연구자 유의사항

- Yellow 기술로 안내받은 경우, 특정 조건에서 보안조치가 적용될 수 있음을 이해
- 기술 등급 또는 보안 검토 결과에 따라 접근 권한이 변경될 수 있음을 인지

가상사례 ❸ 논문에 빠진 한 줄 : 외국 자금 누락의 교훈

개요

- J박사는 한국의 L대학교에 소속된 연구자로, 미국 에너지부(DOE) 산하 국립연구소와 CRADA 체결에 따른 공동연구를 수행. 해당 연구는 DOE의 연구비 지원을 받아 수행되었으며, J박사는 제1저자로 국제 학술지에 공동연구 결과를 발표함
- 그러나 논문 게재 이후, 연구성과에 일부 기여한 외국의 재원이 적절히 표기되지 않았다는 외부 문의가 있었고, 이에 따라 관련 기관은 해당 연구의 자금 출처 명시 여부에 대해 검토를 진행

※ (참고) 본 사례는 현행 규정 등을 바탕으로 창작한 가상의 시나리오이며, 특정 기관이나 실제 사건과는 무관

적용 가능 규정 예시

규정/지침	주요 내용
DOE O 483.1B	체결된 CRADA 내 연구활동과 관련하여 제안된 서면 및 구두 출판물을 사전에 제출해야 하고, 이의를 제기하지 않는다는 서면 답변을 받아 놓을 필요
DOE P 485.1A	외국 재정·기술 협력은 투명하게 공유되어야 하며, 공동연구 시 Disclosure가 요구됨
NSPM-33 Implementation Guidance	논문·특허·성과 발표 시 모든 연구비·자금·기여 요소의 공개 요구를 포함

연구보안 이슈

- 본 사례는 성과물 발표 전 연구비 출처 및 외부 지원에 대한 공개가 불충분했던 경우에 해당하며, 미국 연방정부 자금이 포함된 연구에서 투명성과 연구 무결성의 원칙을 충실히 이행하는 것의 중요성을 강조
- 협력 정보 누락은 의도와 관계없이 신뢰 부족으로 해석될 수 있는 요소로, 협력 기관 간의 조율 부족, 자금 출처의 경계 불명확성 등도 복합적으로 작용 가능

연구자 유의사항

- 논문, 특허, 보고서 등 모든 연구성과물에는 내·외국 자금 출처를 명시하는 것이 원칙임
- 보안 관련하여 자금 출처 등의 외부 비공개를 요청받은 경우에는 철저하게 비공개 필요
- 연구자의 성과물에 외부 자금 및 협력 내용을 누락 없이 반영할 수 있도록 사전 준비 권장

가상사례 ④ 외국 참여자 명시 누락, 공동 제안서의 아쉬운 결과

개요

- W교수는 한국 X대학교 소속으로, 미국 Y대학교와 함께 NASA 연구 과제에 공동 제안서를 제출. 이 제안은 Y대학교가 주관기관(Lead Institution)으로 참여하고, W교수는 공동연구자(Co-Investigator)로 협력할 예정이었음
- 그러나 NASA의 제안서 검토 과정에서, W교수가 현재 특정 외국 공공기관에서 겸직 직위를 보유 중이라는 사실이 사전 Disclosure 문서에 누락되어 있었음
- 제안서 본문에서도 'Foreign Participation' 항목의 기술이 생략되어 있었으며, 해당 외국 협력자의 역할, 기술 접근 범위, 소속 기관의 특성 등이 명확히 기술되지 않은 것으로 확인됨

※ (참고) 본 사례는 현행 규정 등을 바탕으로 창작한 가상의 시나리오이며, 특정 기관이나 실제 사건과는 무관

적용 가능 규정 예시

규정/지침	주요 내용
NASA GCAM (2025년 3월판)	외국 협력자의 참여 여부, 역할, 자원 접근 범위, 소속기관의 특성 등은 명확하게 기술해야 함
NASA FAR Supplement (2025년 1월판)	NASA 지원 과제에 포함되는 외국 연구자 및 기관은 전 단계에서 명확한 Disclosure가 요구됨
NPR 1080.1B Chapter 3	

연구보안 이슈

- 본 사례는 특정 외국 협력자의 정보 누락이 제안서의 절차적 완성도 미비로 해석되어 향후 평가 배제 등 불이익 사유가 될 수 있음을 보여줌
- NASA는 외국 국적자의 과제 참여 시, 단순 명시를 넘어서 협력자의 역할, 기술 접근 권한, 기관의 성격(공공/민간), 기타 관련 요소에 대한 명확한 설명과 형식적 요건 충족을 요구
- Disclosure가 미비하거나 부정확한 경우, 보안 리스크보다는 연방 기관의 과제 제안 절차상 요건 미이행으로 간주되어 행정적 제재 또는 불이익이 발생할 수 있음

연구자 유의사항

- NASA 과제에 제안자로 참여할 경우, 특정 외국 국적자 또는 외국 기관이 포함될 경우 관련 사항을 공개
- 특정 외국인 연구자의 역할 및 기술 접근 범위가 민감 분야에 해당될 수 있으므로, 사전 조율이 필요한 경우에는 미국 측 협력 기관과 함께 사전 검토 권장

가상사례 ⑤ 협력 과정에서의 정보 공유 요청과 기술 보안 검토의 균형

개요

- 한국의 B대학교 소속 N교수는 미국 국립연구소와 CRADA 체결에 따라 공동으로 소재 관련 연구개발(R&D) 과제를 수행. 이 과제는 DOE의 지원 프로그램 중 하나로, 연구 후반에는 시제품 생산 공정 일부에 대한 해석과 시뮬레이션도 포함
- 미국 국립연구소 측은 해당 정보가 기술적 민감도에 따라 보안 관련 평가 대상이 될 수 있으며, DOE의 기술이전 및 수출통제 정책에 따라 외국인 연구자의 정보 접근에는 제한이나 사전 승인 절차가 요구될 수 있다는 점을 사전에 안내
- 그러나, 과제 수행 중 N교수는 실험 조건 재현 및 계산 모델 개선을 위해 민감한 정보로 분류된 특정 문서 공유를 요청

※ (참고) 본 사례는 현행 규정 등을 바탕으로 창작한 가상의 시나리오이며, 특정 기관이나 실제 사건과는 무관

적용 가능 규정 예시

규정/지침	주요 내용
DOE O 142.3B	외국인의 시설 및 기술정보 접근은 정보 분류에 따라 사전 승인 또는 제한 가능

연구보안 이슈

» 본 사례는 공동연구 중 기술적 민감도에 따른 정보 접근 요청이 발생했을 때, 미국 측 보안 기준 및 정책에 따라 정보 제공 범위 및 절차가 조정될 수 있는 상황을 보여줌

» DOE와의 공동연구에서 한국 연구자는 수출통제 기술 및 민감 정보(CUI 등)의 접근에 제한이 있을 수 있음을 숙지하고 관련 절차를 준수 필요

연구자 유의사항

- DOE와의 공동연구에서 특정 문서는 기술 등급에 따라 제한 정보로 분류될 수 있으므로 해당 문서를 요청하기 전 정보의 보안등급 및 접근 허용범위에 대해 사전 협의 필요
- 모든 정보 요청은 공식 채널과 문서 기반 절차를 통해 이뤄져야 하며, 구두 요청 또는 비공식 전달 방식은 지양

가상사례 ❻ 연구 현장 방문 요청에 대한 협의… 보안 요건 반영한 국제협력 절차의 이해

개요

- Y연구원은 한국의 공공연구기관 소속으로, 미국 DOE 산하 국립연구소와 CRADA 체결 없이 협력 수행 중
- Y연구원은 미국 측 연구시설의 실험환경과 장비 구성을 보다 정확히 이해하기 위해 현장 방문을 요청함
- 그러나 해당 실험구역은 안전성과 보안 수준이 높게 설정된 구역으로, 외국 국적자의 출입에는 관련 규정 및 절차에 따른 제한이 있으며 보안 심사 및 별도 승인이 필요한 구역이었음.

※ (참고) 본 사례는 현행 규정 등을 바탕으로 창작한 가상의 시나리오이며, 특정 기관이나 실제 사건과는 무관

적용 가능 규정 예시

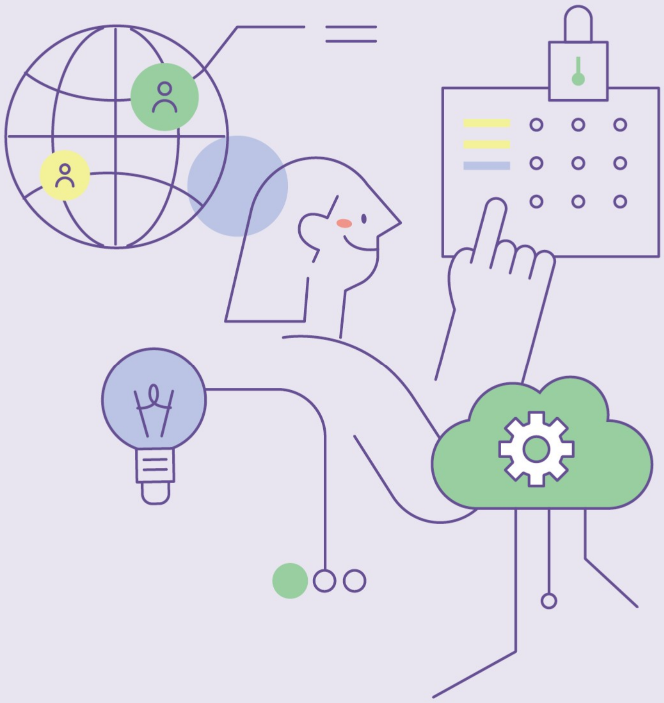
규정/지침	주요 내용
DOE O 142.3B (Foreign National Access Program)	외국 국적자의 DOE 시설 방문 시, 사전 승인 및 보안 절차 이행 필요. 보안 수준이 높은 구역은 별도의 심사 절차 적용 가능

연구보안 이슈

- 본 사례는 물리적 실험시설에 대한 접근 보안 요건과 관련된 국제협력 절차에 대한 이해를 요구하는 사례임
- DOE 산하 국립연구소는 시설 특성상 일부 구역에 대해 보안 심사 및 제한 접근을 운영 중이며, 이는 CRADA 체결 등 협력 유형과는 무관하게 모든 외국인에게 적용됨
- 요청이 거절되었거나 제한적으로 승인되더라도, 협력 자체에 대한 불신이 아닌 법령 및 규정상 요구사항의 반영임을 이해하는 태도가 중요함

연구자 유의사항

- 고위험 또는 보안이 요구되는 기술을 포함하는 연구 협력의 경우, 현장 방문 또는 장비 활용 가능 여부가 제한적일 수 있음을 염두에 둘 것
- 방문 요청 전에는 해당 시설의 보안 요건, 방문절차, 등록 시기 등을 충분히 사전 협의하고, 가능한 경우 최소 수개월 전 준비를 시작
- 해당 규정은 CRADA 등 협력 유형과 무관하게 DOE 기술, 정보, 시설 등에 접근하려는 모든 외국인에 적용됨을 유의



참고문헌

참고문헌

과학기술정보통신부. (2024)「국가연구개발사업 국제공동연구 매뉴얼」, 과학기술정보통신부.

Defense Federal Acquisition Regulation Supplement (DFARS). (2021). DFARS 252.204-7012 : Safeguarding covered defense information and cyber incident reporting. https://www.acquisition.gov/

Government of Canada. (n.d.). G7 common values and principles on research security and research integrity. Science.gc.ca. Retrieved April 3, 2025, from https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/international-research-security-resources/g7-common-values-and-principles-research-security-and-research-integrity

National Aeronautics and Space Administration. (2025). NASA Grant and Cooperative Agreement Manual (GCAM), March 2025 Edition. https://www.nasa.gov/

National Institute of Standards and Technology. (2021). NIST Special Publication 800-171 : Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://csrc.nist.gov/

National Institutes of Health. (2019). Reminders of NIH policies on other support and on policies related to financial conflicts of interest and foreign components (Notice No. NOT-OD-19-114). https://grants.nih.gov/

National Science Foundation. (2024). NSF Proposal & Award Policies and Procedures Guide (PAPPG) 24-1. https://www.nsf.gov/pubs/policydocs/pappg24_1/index.jsp

Office of the Under Secretary of Defense for Research and Engineering. (2019, March 20). Actions for the protection of intellectual property, controlled information, key personnel and critical technologies.

Office of Science and Technology Policy. (2022). Guidance for implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development. https://www.whitehouse.gov/wp-content/uploads/2022/01/NSPM-33-Implementation-Guidance.pdf

Office of Science and Technology Policy. (2022). Guidelines for research security programs at covered institutions. https://www.whitehouse.gov/wp-content/uploads/2022/01/Research-Security-Program-Guidelines.pdf

Sargent, J. F., & Gallo, M. E. (2024, March 27). Federal research and development (R&D) funding:FY2025 (CRS Report No. R48307). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R48307

U.S. Code of Federal Regulations. (n.d.). 32 CFR Part 2002 – Controlled Unclassified Information. https://www.ecfr.gov/current/title-32/part-2002

U.S. Congress. (2018). John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1286, 132 Stat. 1636 (2018).

U.S. Congress. (2022). CHIPS and Science Act of 2022, Pub. L. No. 117–167, 136 Stat. 1366.

U.S. Department of Defense. (2023, June 29). Countering unwanted foreign influence in Department–funded research at institutions of higher education. Office of the Under Secretary of Defense for Research and Engineering.

U.S. Department of Education. (2020). Countering unwanted influence in Department–funded research at institutions of higher education. https://www2.ed.gov/

U.S. Department of Energy. (2016). DOE Order 550.1 Change 1 (LtdChg):Official Travel. https://www.directives.doe.gov/

U.S. Department of Energy. (2019). DOE Order 142.3B:Foreign National Access Program. https://www.directives.doe.gov/

U.S. Department of Energy. (2020). DOE Order 483.1B Change 2 : Cooperative Research and Development Agreements (CRADAs). https://www.directives.doe.gov/

U.S. Department of Energy. (2021). DOE Order 481.1E Change 1 : Strategic Partnership Projects (SPPs). https://www.directives.doe.gov/

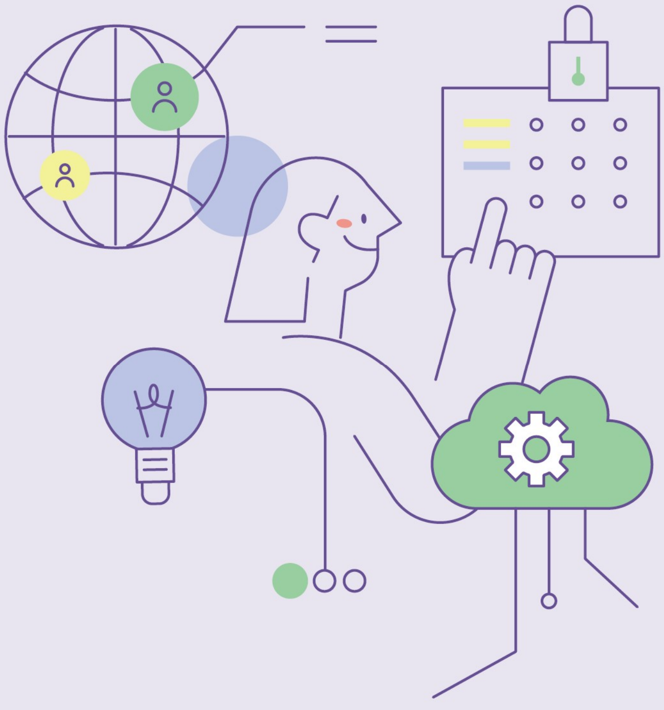
U.S. Department of Energy. (2021). DOE Order 486.1A : Foreign Government Sponsored or Affiliated Activities. https://www.directives.doe.gov/

U.S. Department of Energy. (2021). DOE Policy 485.1A : Foreign Engagements with DOE National Laboratories. https://www.directives.doe.gov/

U.S. Department of Energy. (2022). DOE approach to RTES risk. [Internal guidance document]

U.S. Department of Energy. (2022). Science & Technology Risk Matrix. [Internal guidance document]

부록



(연구자 및 기관용) 국제공동연구 단계별 연구보안 주요 유의사항

<부록> (연구자 및 기관용) 국제공동연구 단계별 연구보안 주요 유의사항

※ 본 부록은 과학기술정보통신부의 「국가연구개발사업 국제공동연구 매뉴얼」('24.2.29.)의 내용을 수정·보완한 것임

1 기획 시 연구보안 유의사항

국외기관 선정 시 보안 유의사항

≫ 국외기관과 공동연구를 추진하거나 연구용역을 위탁하고자 할 경우, 다음의 요건에 해당하면 보안 위험 평가를 실시하고, 기관 내부의 연구보안 전담부서 또는 심의위원회 등을 통해 타당성 검토를 진행하는 것이 바람직

예 검토 기준 대상 예시

- 계약금액이 미화 30만 달러(또는 한화 약 3억 원) 이상인 경우
- 지식재산권의 소유가 국내 연구기관 단독이 아닌 경우
- 상대 기관이 외국 정부, 군사, 정보기관 또는 그 산하 기관과 관련되어 있는 경우
- 상대 기관이 전략물자 통제 대상국 또는 국제 제재 대상국에 소재하거나, 해당 국가의 영향력 하에 있는 경우
- 과거 기술유출 사고 이력 또는 신뢰성 부족이 공식 문서나 언론보도로 확인된 경우

예 검토 항목 예시

- 상대 기관의 법적 성격 및 소유 구조(정부기관 여부, 국유기업 여부 등)
- 연구 범위 및 공유되는 기술의 민감도
- 정보 보호 체계 및 비밀 유지 이행력
- 과거 협력 실적 및 보안사고 유무
- 파트너십 해지 시 대응방안(지식재산 회수 가능성 등)

예 실무 절차 예시

- **[1단계]** 연구책임자가 개요서 또는 제안서 작성 시 국외기관 참여 여부 및 위 조건 충족 여부 사전 체크
- **[2단계]** 기관 내부 보안담당 부서에 사전 검토 의뢰서 제출
- **[3단계]** 보안 전담부서 또는 연구보안 심의위원회에서 검토 후 승인 또는 조건부 승인
- **[4단계]** 협력 추진 시 보안계획서 제출 및 연구보안 준수 서약 체결

비밀유지계약(NDA) 체결 시 유의사항

≫ 공동연구 추진에 앞서, 민감 정보 교류를 수반할 가능성이 있는 경우 반드시 비밀유지계약(NDA, Non-Disclosure Agreement)을 체결해야 하며, NDA의 내용은 다음과 같은 사항을 포함해야 함

비밀유지 의무 범위 확대

- 상대방 기관의 '직원'뿐 아니라, 피용자, 대리인, 재수탁자, 재수탁자의 피용자 및 대리인까지 포괄하여, 이들이 비밀정보에 접근하거나 이를 유출할 가능성이 없도록 제도적 장치 마련

비밀유지서약서 징구 의무 부과

- 위 제3자들로부터 별도의 비밀유지서약서를 징구하도록 상대방 기관에게 계약상 의무를 부과함으로써, 실제적인 구속력을 확보할 수 있음

예 NDA 주요 조항 예시

- 비밀정보의 정의와 범위 (문서, 구두, 전자정보 등)
- 비밀정보의 보관 방식 및 열람 제한
- NDA 위반 시 손해배상 및 법적 책임 조항
- NDA의 유효기간 (연구 종료 후 일정 기간까지 포함)
- 제3자 공유 제한 조항 및 의무 위반 시 통지 절차

보안과제 분류 가능성 사전 검토

연구기획 초기 단계에서 해당 과제가 향후 보안과제 등으로 분류될 가능성이 있는지를 예측하고, 이에 따라 연구 수행 방식을 사전에 설계해야 함

- 국가연구개발사업 보안대책을 적용받는 중앙행정기관의 장은 연구개발결과에 따라 보안과제 여부가 달라질 경우 혁신법 제12조 제2항에 따른 최종평가 시 보안과제 분류의 적정성 검토 가능(보안대책 제14조 제1항)

예 보안과제 분류 가능성 관련 검토 기준 예시

※ (출처) 국가연구개발혁신법 시행령 제45조 제1항

- 「방위사업법」 제3조제1호에 따른 방위력개선사업과 관련된 연구개발과제
- 외국에서 기술이전을 거부하여 국산화를 추진 중인 기술
- 중앙행정기관의 장이 보호의 필요성이 있다고 인정하는 미래핵심기술
- 산업기술의 유출방지 및 보호에 관한 법률」 제2조제2호에 따른 국가핵심기술
- 「대외무역법」 제19조에 따른 수출허가 등 제한이 필요한 기술

기타 사전 점검사항

해외 현지 법률 및 수출통제 규정 확인

- 공동연구 대상국이 수출통제법(ITAR, EAR 등) 또는 연구안보 관련 법률을 적용 중인 경우, 국내법과 충돌하거나 제약이 발생할 수 있으므로 사전 법률 검토 필요

연구기획 문서 내 보안항목 포함 권고

- 연구제안서 및 연구개요서에 '연구보안 계획' 항목 추가
- NDA 체결계획, 보안등급 가이드라인 준수 여부, 참여기관 검토 결과 등 기재

2 계약 시 연구보안 유의사항

계약서 작성 시 보안 유의사항

» 연구계약 체결 시 다음 사항들을 포괄적으로 고려하여 계약 내용에 반영해야 하며, 필요시 기관의 법무팀 또는 외부 법률 전문가의 검토를 거치는 것이 바람직함

» 주요 보안 관리 요소(6가지)

- 계약서 작성 시 아래의 핵심 보안 관리 항목을 포괄적으로 고려할 필요

보안 관리 항목	내용
지식재산권의 귀속 및 보호조치	• 연구성과물의 소유 주체 명시 (단독소유/공동소유/이전 등) • 개량발명, 파생기술에 대한 권리 귀속 범위 • 특허 출원 전 정보 비공개 조항
비밀유지조항	• 정보의 범위 정의(문서, 대화, 디지털 파일 등) • NDA 별도 체결 여부 및 계약서 내 비밀유지기간 설정 • 제3자 공유 제한 및 보안조치 의무
성과물의 발표 및 공개 제한	• 논문, 보고서, 학회 발표 등 사전 협의 의무 • 발표 전 기관 내부 보안 검토 절차 명시
기술이전 및 해외이전 제한	• 기술이전 또는 시제품 이전 시 사전 승인 조건 • 외국으로의 자료 전송 시 암호화 및 승인 절차 의무화
참여연구원 등 인력 변경 제한	• 주요 연구인력 변경 시 사전 통보 및 승인의무 • 외부 인력 활용 시 보안교육, 서약서 징구 명시
계약 해지 및 위반 시 조치	• 보안위반 시 손해배상 및 법적 책임 조항 • 계약 해지 사유로 '보안의무 위반'을 명시

» 기타 권장 조항

- 정보보호 관련 국내·국제 법령 준수 의무
- 연구비 집행 내역의 투명성 확보 조항
- 자료관리 및 연구노트 유지 의무
- 계약 종료 후에도 일정 기간 동안 비밀유지 지속

국제공동연구 계약 시 특별 유의사항

» 해외기관과의 계약에서는 국가별 법률 차이로 인해 분쟁이 발생할 가능성이 있으므로, 특히 다음 사항을 신중히 점검

» 관할 법원 및 준거법 명시

- 분쟁 발생 시 적용될 국가 법률과 재판 관할권을 명확히 합의해야 함

※ (예시) "본 계약은 대한민국 법률을 준거법으로 하며, 모든 분쟁은 서울중앙지방법원을 관할 법원으로 한다."

» 수출통제 관련 조항 포함

- 미국, EU 등 수출통제법(ITAR, EAR, Dual-use regulation 등)의 적용 가능성이 있는 기술에 대해서는 수출허가 및 관련 의무를 계약에 명시

» 비밀유지 위반 시 실질적 제재방안 확보

- 해당 국가에서 계약의 강제력과 손해배상 효력이 있는지를 법률 검토 후 계약서에 반영

» 다국어 계약서의 해석 기준 명확화

- 계약서가 한글 및 외국어로 작성되는 경우, 해석 상 충돌 발생 시 기준 언어를 지정

※ (예시) "한글본과 영문본 사이에 해석 차이가 발생할 경우, 한글본을 우선으로 한다."

성과의 소유 및 활용 관련 조항

» 연구성과에 대한 소유권과 활용 조건을 사전에 명확히 정의하고, 불필요한 외부 공개나 기술유출을 방지하기 위한 선제적 조치 필요

예 지식재산권(IPR) 관련 조항 예시

- "본 연구의 결과로 발생한 모든 지식재산권은 ○○ 기관이 단독으로 소유한다."
- "해당 기술은 외국기관에 이전할 수 없으며, 특허출원 전 외부에 공개할 수 없다."
- "성과물의 활용 시 상대기관은 사전에 서면 승인을 받아야 한다."

» 비밀특약 조항 활용

- 연구성과 중 공개 여부가 불분명한 성과에 대해서는 비밀특약 조항(Confidential Annex) 을 별도로 설정하여 민감정보 유출을 방지

계약 체결 시 실무 프로세스

단계	내용	담당자
① 계약 초안 검토	연구책임자와 법무팀이 주요 조항 검토	연구책임자, 법무담당
② 보안조항 점검	NDA, IPR, 보안이행 조항 포함 여부 확인	보안담당자
③ 기관 승인	기관 내 보안심의 또는 법률검토 승인 절차	기관장, 보안위원회
④ 최종 체결	쌍방 서명 및 원본 보관	계약담당 부서

3 수행 중 연구보안 유의사항

보안대책의 이행 및 관리

- 연구기관은 연구자 개인의 자율적 보안 준수를 장려하는 동시에 조직적·체계적인 보안관리 시스템을 구축하여 연구보안이 내재화되도록 지원 필요

예 주요 이행 항목 예시

- 연구자 대상 정기적인 보안교육 실시 (연 1회 이상)
- 국제공동연구 수행 전 서약서 제출 및 사전교육 의무화
- 외부기관 방문 전 사전보고 및 기관 내부 승인 절차 운영
- 연구성과물 외부 공개 전 보안담당자 사전검토

예 시나리오별 보안 조치 예시

상황	보안 조치
국제학회 참석	참석 전 기관 승인 → 발표자료 보안 검토 → 비밀정보 포함 여부 점검
공동연구 파견근무	파견 전 서약서 작성 → 파견지 보안환경 확인 → 정보접근 제한 설정
외부 발표 또는 언론 인터뷰	발표 내용 사전 제출 → 비공개 정보 존재 여부 확인 → 보안 책임자 승인 후 발표
내부 회의 중 외부인 참여	회의 초청 명단 사전 등록 → 외부인 신분 확인 및 제한 구역 접근 금지 조치

예 보안 이행 점검 항목 예시

- 연구 시작 전 보안서약서 징구 여부
- 참여자 대상 보안교육 이수 여부
- 연구정보 공유 시 암호화·접근권한 제한 적용 여부
- 연구성과물에 대한 공개 전 검토 프로세스 존재 여부
- 외부 협력자와의 자료 공유 시 NDA 유효 여부

연구노트 작성 및 보안관리

- 연구노트는 연구자의 아이디어, 실험결과, 성과 분석 등이 기록되는 자료로, 지식재산권 분쟁 시 기여도를 입증하고, 보안자료로서의 법적 근거가 될 수 있으며, 「국가연구개발혁신법」 제35조 및 시행령 제65조 제1항에 따라 체계적인 작성과 보관이 요구됨
- 연구노트 작성 지침
  - 연구개발의 진행 과정과 결과를 일자별로 작성

- 공동 실험의 경우, 각 연구자의 기여도 명확히 기재
- 실험과정 중 변경사항, 중단 사유 등도 모두 기록
- 타인의 서명·날인 또는 디지털 서명 등 검인 절차 포함 권장

» 보관 지침 및 보안수준

- 잠금장치가 있는 서랍 또는 문서보관함에 물리적 보관
- 스캔하여 전산화(백업)하고 접근권한을 제한
- 최소 5년 이상 보관 권장 (기관 규정에 따름)
- 연구 종료 후에도 연구성과 관련 분쟁 우려 시까지 폐기 금지

예 연구노트 관련 FAQ 예시

Q1 공동연구자인 외국 파트너와 연구노트를 공유해도 되나요?

A1 외국기관과의 연구노트 공유는 NDA 체결 여부, 보안등급, 정보 민감도 등을 고려해 제한적으로 허용되어야 하며, 기관 보안담당자 승인 후 가능

Q2 연구노트는 디지털만으로도 충분한가요?

A2 전자연구노트도 유효하나, 접근권한 관리, 위변조 방지, 백업 체계가 충실해야 하며, 기관은 이를 별도 보안관리 체계로 관리해야 함

보안등급 재분류 및 수행 중 보안사항 변경 시 대응

» 연구개발기관의 장은 수행 예정이거나 수행하고 있는 보안과제에 대하여 재분류가 필요하다고 판단하는 경우에는 보안과제분류위원회에 보안과제 여부를 재분류해줄 것을 요청할 수 있음

※ (근거) 「국가연구개발사업 보안대책」 제3조 제2항

- 연구 수행 중 과제 성격 또는 외부 환경 변화로 인해 과제가 보안과제 등으로 분류되거나 보안등급이 상향·하향될 수 있으므로 관련 규정에 따라 적시에 재분류하고 관련 보안조치를 강화 또는 완화 필요

» 보안등급 재분류 절차

※ 「국가연구개발사업 보안대책」 제14조 제1항 기준

- 연구책임자 또는 기관이 보안등급 변경 필요성 인지
- 소관 중앙행정기관(부처)의 보안담당 부서에 보안등급 재분류 요청
- 「국가연구개발혁신법」 제12조 제2항에 따른 최종평가 시 적정성 검토
- 등급 변경 후 보안계획서 수정 및 추가 보안조치 이행

연구자 및 실험실 보안 문화 정착

예 연구자 차원의 실천 항목 예시

- USB 등 저장장치 무단 반출 금지
- 연구자료 이메일 전송 시 암호화 및 수신자 확인
- 실험실 내 외부인 출입 기록 및 감시
- 공동 컴퓨터 로그인 기록 정기 점검
- 출퇴근 시 연구자료 잠금, 모니터 자동잠금 설정

예 기관 차원의 운영 권고사항 예시

- 연구실별 보안관리책임자(RSO, Research Security Officer) 지정
- 보안사고 발생 시 대응 매뉴얼 마련 및 모의훈련 실시
- 정기적인 보안감사 및 연구책임자 대상 인터뷰

4 종료 후 연구보안 유의사항

특허출원 시 보안 유의사항

- 연구성과가 특허로 이어질 경우, 특허출원 전·후 과정에서 보안 리스크를 사전에 차단 필요
- 특허사무소 선정 및 계약 시 보안조치
  - 특허출원을 대행하는 외부 특허사무소와 비밀유지계약(NDA) 체결
  - 사무소 임직원 대상 보안서약서 징구
  - 기술문서 송수신 시 보안메일 또는 암호화 전송 시스템 사용
  - 국내외 특허출원 동시 진행 시, 국가별 민감도 고려하여 공개 여부 결정
- 출원 전 보안 검토 프로세스 예시
  - 연구책임자 → 기관 보안담당자에게 출원 요청
  - 보안담당자 → 기술 민감성 및 대외 공개 가능 여부 검토
  - 민감기술 포함 시, 외부 공개를 제한하거나 비밀특허 제도 검토
  - 기관장 또는 연구보안위원회 승인 후 출원 진행
- 비밀특허제도 활용 권고
  - 전략기술이나 국방·안보 관련 기술의 경우, 일정 기간 비공개 상태로 특허를 보호할 수 있도록 비밀특허제도 활용 고려
  - (국내 기준) 국가안보에 영향을 미치는 경우, 지재권 전담기관과 협의 후 비공개 유지 요청 가능

논문 게재, 학회 발표 등 대외 공개 시 보안검토

- 논문, 보고서, 학회 발표 등 연구성과의 공개는 필수적인 학문적 활동이지만, 보안 위험요소가 내재하므로 다음 절차를 준수
- 사전 공개 검토제 운영 권장
  - 기관 차원에서 "성과 공개 전 보안검토 제도" 마련
  - 학술지 투고 전, 사내 보안담당자 또는 기술보호위원회의 기술 민감도 점검 필수
  - 외부 학회 발표 자료는 반드시 사전 승인 절차를 거쳐야 함
- 학회 발표 시 유의사항
  - 발표자료에 민감기술, 공동개발 중인 비공개 기술 포함 금지
  - 질문응답 과정에서 비계획적 정보 유출 방지 교육 필요
  - 온라인 컨퍼런스 참여 시, 화면 공유·채팅 유출 등의 기술적 리스크 관리

예 기술 내용 검토 체크리스트 예시

- 국가전략기술 포함 여부 확인
- 외국 정부 또는 기업과의 공동 성과 여부 검토
- 미출원 특허내용 포함 여부
- 산업적 활용 가능성이 큰 핵심기술 포함 여부

기술이전 및 사업화 시 보안조치

» 연구성과를 기업 등에 기술이전하거나 사업화할 경우, 경제적 가치뿐 아니라 보안의 관점에서도 철저한 검토 필요

» 기술이전 계약 시 유의사항

- 기술평가서에 보안등급, 공개범위, 보유기술의 전략성 명시
- 이전 대상 기업과의 NDA 및 활용제한 조항 삽입
- 기술이전 후, 재이전 금지 및 타인에게의 공개 제한 조항 포함
- 기술 활용 목적 외 사용 금지 및 위반 시 벌칙 조항 명시

» 수출통제 기술 포함 여부 검토

- 이전 기술이 전략물자에 해당하거나 수출통제대상에 포함되는 경우, 산업통상자원부 등 관계기관 협의를 통해 사전 허가 획득
- 외국기업 또는 합작법인 이전 시, 기술보호심의 필요

성과활용 단계에서의 연구보안 관리체계 운영

» 보안책임자 승인제 운영 권고

- 성과 발표, 기술이전, 특허출원 등 외부 활용 전 반드시 부서장 또는 보안담당자 승인을 받도록 제도화
- 승인 절차를 전산화하여 기록을 남기고, 이행 내역 정기 점검

» 성과활용 보안절차 통합 가이드 배포

- 연구성과 활용 시점별로 필요한 보안조치, 문서 양식, 책임자 역할을 명시한 성과활용 보안매뉴얼을 제작·배포

» 성과활용 이후 추적관리

- 기술이전 후 일정 기간 동안 활용 현황 보고 의무 부과
- 민감 기술의 경우, 타기관 재이전 또는 해외 이전 발생 시 사후보고 체계 운영

<색인> 주요 용어 해설

용어	정식 명칭	정의 및 설명
ACP (NASA)	Access Control Plan	• **NASA 시설, 정보, 기술에 접근하려는 외국인 또는 외부기관이 충족해야 할 보안 및 수출통제 요건을 규정하는 문서.** 보안성, 수출통제 적합성, 승인 절차 등을 종합적으로 관리함
BIS	Bureau of Industry and Security	• **미국 상무부 산하 산업안보국.** 수출통제(EAR) 및 전략물자 관리 담당 기관
CI	Counterintelligence	• **방첩.** DOE 내에서는 외국의 정보활동, 산업스파이, 기술유출 등을 탐지·방지하기 위한 정보보안 활동을 의미함. DOE 방첩국(DOE-IN)이 이를 총괄하며, 외국인 접근심사, 방첩 브리핑 등을 수행함
COA	Collaborators and Other Affiliations	• **NSF 연구제안서 제출 시, 심사위원과의 이해충돌을 피하기 위해 제안자의 공동연구자, 지도교수, 제자 등 협력관계자 목록을 명시하는 필수 문서**
CRADA	Cooperative Research and Development Agreement	• **협동연구개발계약.** DOE 국립연구소와 외부 기관(산·학·연 포함)이 공동연구를 수행할 수 있도록 하는 공식 계약 형태
CSO	Cognizant Secretarial Office	• **DOE(미국 에너지부) 내에서 특정 프로그램, 사업, 연구개발 분야를 책임지고 관리·감독하는 주무 차관보(Assistant Secretary) 조직 또는 사무국을 의미.** 특정 외국인 접근 요청, 민감 주제(Sensitive Subject) 접근, 외국 협력 검토 등과 관련해, 해당 분야를 관할하는 CSO의 검토 및 승인이 필요한 경우가 있음.
CUI	Controlled Unclassified Information	• **통제 비분류 정보.** 기밀은 아니나 외부 공개가 제한되는 중요 민감 정보로, 특별한 접근통제 및 보호조치가 요구됨
DAEO	Designated Agency Ethics Official	• **지정 윤리책임관.** DOE 내 각 기관 또는 부서에서 공무원의 이해충돌, 외국 정부 연계 활동 등을 심의하는 윤리 담당자
DDTC	Directorate of Defense Trade Controls	• **미국 국무부 방위무역관리국.** 무기수출관리(ITAR) 관련 규정 및 허가 담당
DFARS	Defense Federal Acquisition Regulation Supplement	• **미국 국방부(DoD)의 연방조달규정.** 방위 계약 관련 규정 집합
DoD	Department of Defense	• **미국 국방부.** 군사 관련 연구개발(R&D) 및 국가안보 연구 수행
DOE	U.S. Department of Energy	• **미국 에너지부.** 국립연구소 운영 및 에너지·과학기술 관련 연구개발(R&D) 정책 총괄 부처로, 연구보안 관련 다수의 규정을 제정·운영
EAR	Export Administration Regulations	• **미국 상무부 BIS가 운영하는 수출관리 규정.** 민수용 이중용도 기술 통제
FACTS	Foreign Access Central Tracking System	• **외국인 접근 중앙 추적 시스템.** DOE 시설, 기술, 정보에 접근하려는 외국인의 정보를 등록·심사·추적하는 시스템으로, 위험국가 출신 여부, 민감 기술 접근 여부 등을 판단하는 보안 통제의 핵심 도구
FCOC	Foreign Countries of Concern	• **우려 국가.** 미국 국무부 또는 관련 법령에 따라 지정된 외국 정부로, 기술유출·인권침해·지식재산 탈취 등의 우려로 인해 연구협력 시 추가적인 검토나 제한 조치가 적용됨.

용어	정식 명칭	정의 및 설명
FCOI	Financial Conflict of Interest	• **연구자의 재정적 이해충돌 문제.** 주로 NIH, NSF 등 연구지원기관 규정에서 요구
FGTRP	Foreign Government Talent Recruitment Program	• **외국 정부가 운영하는 인재유치 프로그램.** 기술유출 가능성 등으로 인해 미국 내 공공기관 연구자의 참여가 금지됨
FOAB	Field Operations Advisory Board	• **DOE 본부(HQ) 소속의 자문기구**로, 국제협정 체결 등에서 **위험국가 또는 민감 기술 관련 사안에 대한 사전 검토**와 의견 제시를 수행
FOCI	Foreign Ownership, Control, or Influence	• **외국 소유·지배·영향 여부.** 연구기관 또는 기업이 외국 이해관계에 의해 통제되거나 영향을 받을 가능성을 판단하는 보안 심사 항목
FTMS	Foreign Travel Management System	• **외국출장 관리 시스템**. DOE 직원 및 계약자가 해외출장(official foreign travel)을 계획하거나 수행할 때 사용하는 내부 시스템으로, 출장 목적·일정·접촉 대상 등을 입력하고, 보안심사, 방첩 브리핑, 승인을 연계함. DOE O 550.1(Official Travel)에 근거
GC	Office of the General Counsel	• **법무실.** DOE의 법률 자문기관으로, 법령 해석, 규정 제정 지원, 계약·소송 대응, 윤리·보안 관련 법률 검토 등의 기능을 수행함
GCAM	Grant and Cooperative Agreement Manual	• **NASA가 외부 기관과 체결하는 보조금(Grant) 및 협력계약(Cooperative Agreement)을 관리하는 공식 실무 매뉴얼.** 계약 체결, 재정관리, 성과보고, 종료 절차까지 포괄적으로 규정.
IA	Interagency Agreement	• **정부기관 간 협정(기관 간 계약).** DOE와 다른 미국 연방기관(예 : NASA, DoD, NIH 등)이 자금이나 기술, 서비스를 상호 제공하기 위해 체결하는 협정 형태. SPP와 달리 외부 민간이 아닌 정부 간 협력에 해당함. DOE가 외부 업무를 대행하거나 지원받는 구조에서 사용
IAEA	International Atomic Energy Agency	• **국제원자력기구.** 원자력의 평화적 이용 및 비확산 관련 국제기구
IN (DOE-IN)	Office of Intelligence and Counterintelligence	• **DOE 정보·방첩국**. 외국인 접근 심사, 인덱스 조회(Indices Checks), 방첩 브리핑 등 연구보안의 정보보안 분야를 총괄
ITAR	International Traffic in Arms Regulations	• **미국 국무부 방위물자 수출통제 규정.** 군사물자 및 관련 기술 통제
JIT	Just-In-Time (정보 제출)	• NIH 등 연구기관에서 과제 심사 직전 필요한 추가 서류 요청 시 **적시 제출을 뜻하는 단어**
LOI	Letter of Intent	• **의향서.** DOE와 외부 기관 간 협력 추진을 위한 비구속적 합의 문서로, 정식 계약(CRADA, SPP, MOU 등) 체결 전 상호 관심사항을 명시하여 협력 방향을 사전 조율함.
MFTRP	Malign Foreign Talent Recruitment Program	• **악의적 외국 인재유치 프로그램.** FGTRP 중에서도 특히 위험성이 큰 것으로 지정된 프로그램
NASA	National Aeronautics and Space Administration	• **미국 항공우주국.** 우주 탐사 및 항공과학 연구기관
NDA	Non-Disclosure Agreement	• **비밀유지계약.** 공동연구 또는 기술교류 과정에서 취득한 민감정보(기술, 데이터, 지적재산 등)의 무단 공개를 방지하기 위해 체결하는 법적 계약
NFS	NASA Federal Acquisition Regulation Supplement	• **NASA 전용 연방조달규정**

용어	정식 명칭	정의 및 설명
NISPOM	National Industrial Security Program Operating Manual	• **미국 국방부 주관 국가산업보안 운영지침.** 방위산업체 보안규정
NIST	National Institute of Standards and Technology	• **미국 국립표준기술연구소.** 과학기술 표준·보안 가이드라인 제정기관
NNSA	National Nuclear Security Administration	• **DOE 산하 국가핵안보청**. 핵무기 관리, 핵비확산, 국방 관련 핵기술을 담당하며 보안이 특히 강화된 연구기관 운영
NPR	NASA Procedural Requirements	• **NASA의 정책(NPD)을 실무적으로 집행하기 위한 절차 지침 문서.** 프로그램 관리, 연구과제 수행, 보안, 재정관리 등 모든 NASA 활동에 필수적으로 적용됨.
NSPM-33	National Security Presidential Memorandum-33	• **미 백악관이 발표한 국가연구보안 대통령교서.** 연구자 국외관계 보고 및 보안 정책 강화 지침 등을 명시
NSF	National Science Foundation	• **미국 국립과학재단.** 비군사 기초과학 연구 지원 주무기관
NSF OIG	National Science Foundation Office of Inspector General	• **NSF 감사실.** NSF 산하의 독립 감사·조사기구로, 연구비 부정사용, 연구윤리 위반, 이해충돌 등을 감시·감사하며, 내부고발 및 부정행위 조사를 수행함
PAPPG	Proposal and Award Policies and Procedures Guide	• **NSF의 연구제안서 및 과제운영 절차 가이드라인.** 연구보안 요건도 포함
PSO	Program Security Officer	• **DOE 및 국방부 등에서 프로그램별 보안책임자로 지정된 인물**
RPPR	Research Performance Progress Report	• **연방연구지원 과제의 중간성과 및 진척상황을 보고하는 표준 양식**
SciENcv	Science Experts Network Curriculum Vitae	• **미국 연구자 이력서 통합시스템.** NSF, NIH 등에 이력서 제출 시 사용
SCL	Sensitive Countries List	• **민감국가 목록.** DOE가 핵 비확산, 경제안보, 테러지원 등을 고려해 정책적으로 지정
SPP	Strategic Partnership Projects	• **전략적 파트너십 프로젝트**. DOE가 민간·외부 기관과 전략적 목적으로 공동 수행하는 프로젝트. 보안 및 임무 부합성 심사 필수
SSP	System Security Plan	• **정보시스템의 보안통제 및 보호조치 현황을 상세히 설명하는 공식 문서.** NIST 가이드라인에 따라 민감정보(CUI 등)를 다루는 모든 기관과 계약자는 SSP 작성·유지가 필수
SST	State Sponsor of Terrorism	• **미국 국무부가 지정한 국제 테러 지원국.** DOE를 비롯한 모든 미국 정부기관의 연구보안, 외국인 관리, 수출통제 정책에 있어 가장 높은 수준의 제한 조치를 적용받음.
TCP	Technology Control Plan	• **기술통제계획.** 수출통제 대상 품목(기술, 데이터, 장비 등)의 보호를 위해 접근통제, 책임자 지정, 위반 대응 등을 규정하는 공식 보안 계획 문서.
TTCP	Technology Transfer Control Plan	• **기술이전 통제계획.** 민감기술의 이전 과정에서 제3국 유출 방지를 위해 수립하는 보호조치
UCNI	Unclassified Controlled Nuclear Information	• **통제 비분류 핵정보.** 핵무기·핵물질 등과 관련된 정보 중 법적으로 비분류이지만 특정한 통제가 필요한 민감 정보

| 미국편 |

국제공동연구 연구보안

길잡이

과학기술정보통신부
Ministry of Science and ICT

KISTEP 한국과학기술기획평가원
Korea Institute of S&T Evaluation and Planning