STRIDER

SECURING THE FUTURE OF ACADEMIC RESEARCH

NSPM-33 Compliance and Research Security

TABLE OF CONTENTS

INTRODUCTION

Academic institutions are at the forefront of scientific discoveries that shape advanced technology capabilities. While academic institutions have benefited from open and collaborative scientific research, that environment is also vulnerable to foreign interference, exploitation, and security threats.

To ensure U.S.-led open and collaborative research continues to power scientific discoveries in a safe and secure manner, the National Security Presidential Memorandum 33 (NSPM-33) was issued in 2021, establishing research security standards for institutions receiving federal funding.

For universities striving to lead in research innovation while maintaining compliance with these federal mandates, understanding and implementing robust research security measures is essential. This eBook will guide you through the critical components of research security as outlined in NSPM-33, and how your institution can ensure compliance, protect its intellectual assets, and uphold the integrity of its research endeavors.

BACKGROUND: GLOBAL LANDSCAPE

The U.S. and allied nations face unprecedented challenges in protecting their research ecosystems from exploitation from competing nations, particularly by the People's Republic of China (PRC). The PRC's long-term goals of science and technology (S&T) dominance and self-reliance, along with government-driven tactics for recruiting top global talent and accessing cutting-edge S&T, pose risks for Western academic institutions.

While the bulk of global scientific research is conducted for the sake of advancing science, the PRC government views scientific advancement—and global collaboration in particular—as a means to advance national strategic interests. Underscoring this perspective is Xi Jinping's call on scientists to "not forget their original intention, keep the mission firmly in mind, and adhere to the supremacy of the national interest." Xi Jinping also stated that, "Science has no borders but scientists have motherlands."[1] PRC tactics target any person from any national origin with expertise in a field that they deem necessary for self-reliance and national strength.

PRC policies, such as the "Made in China 2025" initiative, aim to bolster China's capabilities in advanced technologies while promoting international collaboration. This approach encourages joint ventures, research partnerships, and expanded knowledge-sharing with foreign organizations. While these collaborations can enhance research by adding diverse perspectives and accelerating innovation, they may also introduce potential risks to U.S. research institutions. These dynamics highlight the need for comprehensive research security measures, as outlined by NSPM-33, to ensure that researchers and their work are protected in an increasingly interconnected research environment.

UNDERSTANDING NSPM-33

What is NSPM-33 and Why Does it Matter?

National Security Presidential Memorandum 33 (NSPM-33) was enacted to enhance the protection of U.S. Government-supported research and development from foreign threats. This directive recognizes that while the U.S. research enterprise thrives on openness and collaboration, these same qualities can also make it vulnerable to exploitation by foreign entities.

NSPM-33 mandates that all institutions receiving significant federal research funding must implement comprehensive research security programs. These programs are designed to address critical areas such as cybersecurity, foreign travel security, insider threat awareness, and export control compliance.

For academic institutions, particularly those leading in research and innovation, compliance with NSPM-33 is not just a legal requirement but a critical step in safeguarding the future of academic research.

Key Requirements for Academic Institutions

Academic institutions play a pivotal role in the U.S. research ecosystem. Under NSPM-33, they are required to develop and implement research security programs that address the following key areas:

CYBERSECURITY

Institutions must protect their research data and intellectual property from cyber threats by implementing robust cybersecurity measures. This includes regular training, controlled access to information systems, and monitoring of communications.

FOREIGN TRAVEL SECURITY

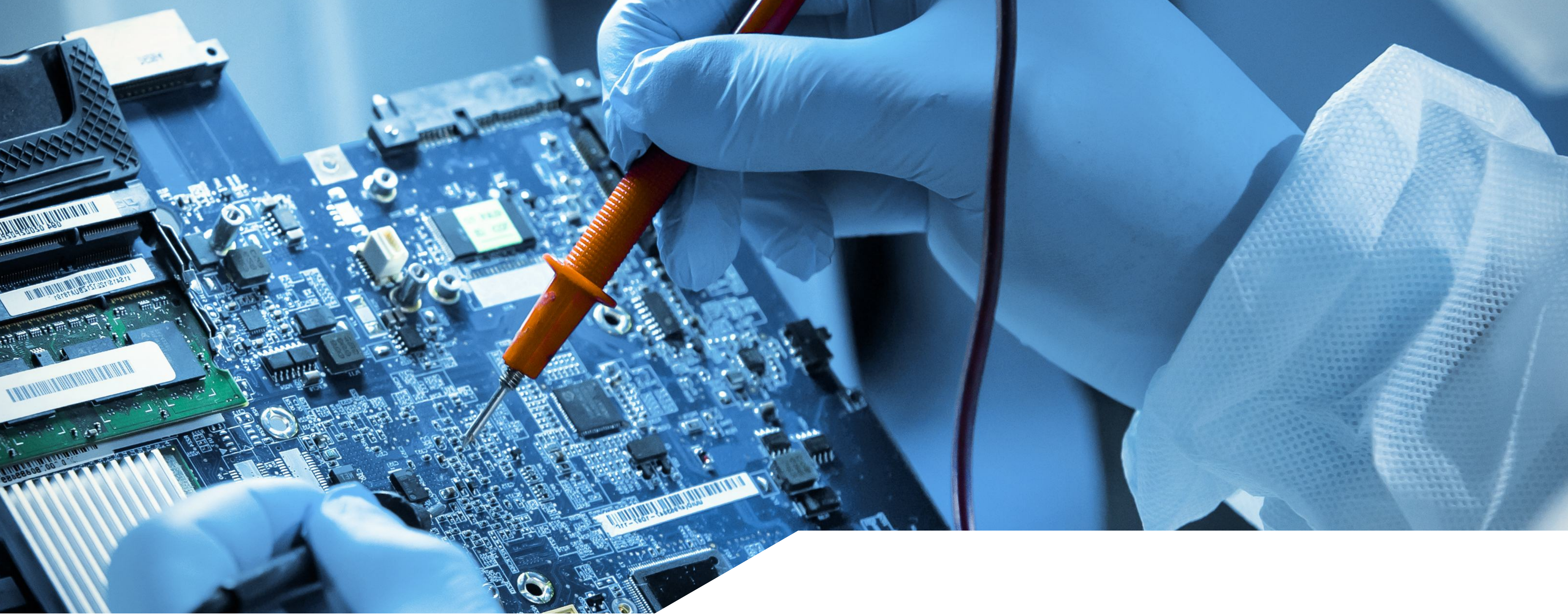
Universities must monitor and secure foreign travel undertaken by faculty and staff. This includes providing security briefings, tracking travel, and ensuring the security of electronic devices used abroad.

RESEARCH SECURITY TRAINING

Institutions are required to train their personnel to recognize and mitigate research security risks, including insider threats. This involves understanding the risks posed by individuals within the organization who may intentionally or unintentionally compromise research security.

EXPORT CONTROL COMPLIANCE

For research involving sensitive technologies, universities must ensure compliance with export control regulations. This includes training on reviewing foreign sponsors and collaborators and adherence to restricted entities lists.



The need for these requirements is underscored by real-world examples of loss of talent, and the transfer of sensitive information. These threats are real and highlight the critical importance of complying with NSPM-33.

By understanding and implementing these key requirements, academic institutions can protect their research endeavors while remaining compliant with federal mandates.

While this eBook primarily focuses on U.S.-based academic institutions and their compliance with NSPM-33, the principles of research security are equally critical for institutions in Canada, Australia, Europe, and Japan, all of which face similar threats and have enacted their own legislation to protect research integrity. This international movement highlights the global nature of research security and the shared responsibility of academic institutions worldwide to protect their research assets.

STRATEGIC RECOMMENDATIONS FOR RESEARCH INSTITUTIONS

Best Practices for NSPM-33 Compliance

To ensure compliance with NSPM-33 and protect the integrity of their research, academic institutions should adopt the following best practices:

01

DEVELOP A COMPREHENSIVE RESEARCH SECURITY PROGRAM

Institutions should establish a dedicated team to oversee the implementation of NSPM-33 requirements. This team should be responsible for developing and enforcing policies related to cybersecurity, foreign travel security, insider threat awareness, and export control compliance.

02

CONDUCT REGULAR TRAINING AND AWARENESS PROGRAMS

Continuous education is key to maintaining compliance. Institutions should conduct regular training sessions for faculty, staff, and students on research security protocols and the importance of adhering to NSPM-33 guidelines. This initiative also builds trust between research security teams and their researchers, leading to collaboration and communication when they're approached or asked to collaborate.

03

IMPLEMENT ADVANCED CYBERSECURITY MEASURES

Protecting research data from cyber threats is a top priority. Institutions should invest in robust cybersecurity technologies, including firewalls, encryption, and monitoring systems, to safeguard their intellectual property.

04

STRENGTHEN COLLABORATION AND COMMUNICATION

Encourage open communication among departments to ensure that all faculty and staff are aware of their roles in maintaining research security. Collaboration between IT, legal, and research departments is essential for a cohesive security strategy.

05

LEVERAGE TECHNOLOGY SOLUTIONS

Utilize technology solutions that automate and streamline compliance processes. This can include software for tracking foreign travel, monitoring insider threats, and verifying disclosures. These tools help ensure that your institution remains compliant with minimal administrative burden. Strider offers a suite of research security solutions designed to secure your institution's people, technology, and talent to maintain compliance with NSPM-33.

Securing Against Risk in Foreign Collaborations

Institutions should be particularly vigilant in monitoring collaborations with foreign entities, as **PRC strategies often include talent recruitment programs and joint research ventures that can lead to unintended data leakage and intellectual property theft.** Implementing thorough verification processes for international affiliations is a critical step in mitigating these risks.

Positioning for Leadership in Research Security

By taking proactive steps to implement these best practices, academic institutions can position themselves as leaders in research security. This leadership not only protects their research but also enhances their reputation in the academic community. As compliance with NSPM-33 becomes increasingly important, those institutions that lead the charge in research security will influence best practices across the sector, ultimately shaping the future of academic research.

THE FUTURE OF RESEARCH SECURITY

The landscape of research security is continuously evolving. As new threats emerge and technology advances, academic institutions must stay ahead of the curve by regularly updating their security measures and compliance protocols. NSPM-33 is just the beginning; the future will likely see even more stringent requirements as the U.S. government continues to prioritize the protection of its research assets.

For institutions committed to maintaining their status as leaders in research and innovation, staying informed about the latest developments in research security is crucial. Institutions must not only comply with existing mandates but also anticipate future requirements by fostering a culture of security awareness and investing in advanced technologies that provide comprehensive protection against emerging threats.

Now is the time for your institution to take the necessary steps to ensure compliance with NSPM-33 and other international regulations and secure its research future.

Schedule a consultation with Strider today to learn how our comprehensive research security solutions can help your institution achieve NSF compliance and protect its most valuable assets.

Schedule a demo →

STRIDER

THANKYOU

striderintel.com