RESEARCH SECURITY MANAGEMENT CERTIFICATE PROGRAM

Course Descriptions

RESEARCH SECURITY MANAGEMENT CERTIFICATE PROGRAM

THE TEXAS A&M
UNIVERSITY SYSTEM
RESEARCH SECURITY OFFICE

CONTENTS

Program Introduction 3

Introduction to Research Security 4

Understanding Insider Threat Risks to Research Programs 5

Illicit Elicitation: Identifying Subtle Attacks on Researchers 6

Get Off the X: Protecting Research Program Assets During Travel 7

Dodging Danger: Understanding Research Program Compliance Issues 8

Certificate Program Presented By 9

RESEARCH SECURITY MANAGEMENT CERTIFICATE PROGRAM

The strategic importance of university, corporate, military and government research programs in the biopharmaceutical, biotechnology, oil/gas/nuclear energy, telecommunications, advanced computing, and other cutting-edge research sectors, make them attractive targets for both outsider and insider threat actors. There is a growing trend of incidents involving the misuse, loss, theft and misappropriation of Intellectual Property (IP), including trade secrets, unpublished research findings, and other research-derived information assets. IP theft and misappropriation remains a significant risk to every research organization. The value and importance of research programs require that everyone associated with a research organization work together to protect the confidentiality, integrity and availability of the research assets created. The Texas A&M University System Research Security Office has developed an innovative approach to safeguard research assets against sophisticated global threats both inside and outside research organizations. The Research Security Office has been recognized as a leader in research data protection and has established best practices that have set the standards in the research security management field.

The Texas A&M University System, in partnership with its Research Security Office, the Texas A&M Engineering Experiment Station, National Center of Therapeutics Manufacturing and Trust Farm LLC, has created a series of courses to educate research program professions on research security issues. The Research Security Management Certificate Program consists of a series of curated online courses to develop academic, corporate, military and government research program knowledge and skills to better manage the security, integrity and compliance landscape of research programs in the United States and beyond.

The overarching goal of the Research Security Management (RSM) courses is to prepare researchers, research program managers, faculty, technicians, staff members, students, licensing and commercialization program leaders, security professionals, compliance officers, regulatory and export control experts, administrators, and executives to effectively identify, assess, investigate and mitigate complex enterprise risks to research programs.

Participants completing the five-course series will be awarded a Research Security Management Certificate by the National Center of Therapeutics Manufacturing (NCTM) and are eligible for Continuing Education Units (CEUs).

The cost of the Research Security Management Certificate Program is only $975. Course registrations are accepted year-round and are available on the NCTM training website.

COURSE #: RSM 301 | NCTM 1301

COURSE TITLE

Introduction to Research Security

OVERVIEW:
An introduction to the theory, practice, challenge and prospects for securing research assets against insider and outsider threats, with special emphasis on how researchers and other research program professionals can lead the protection efforts; provides an overview of the research management practice and introduces basic program concepts to help research program professionals understand the role of research security; provides insights into the internal and external threats facing the security and integrity of research programs, how security program managers assess the likelihood and impact of associated risks, and how best to develop response and resource plans to effectively mitigate those risks to an acceptable level; provides an overview of Confidentiality, Integrity and Accessibility principles of information security and how those principles apply to the overall strategy of a Research Security Management Program.

PREREQUISITE: None
COURSE LENGTH: 60-minutes
FORMAT: Online

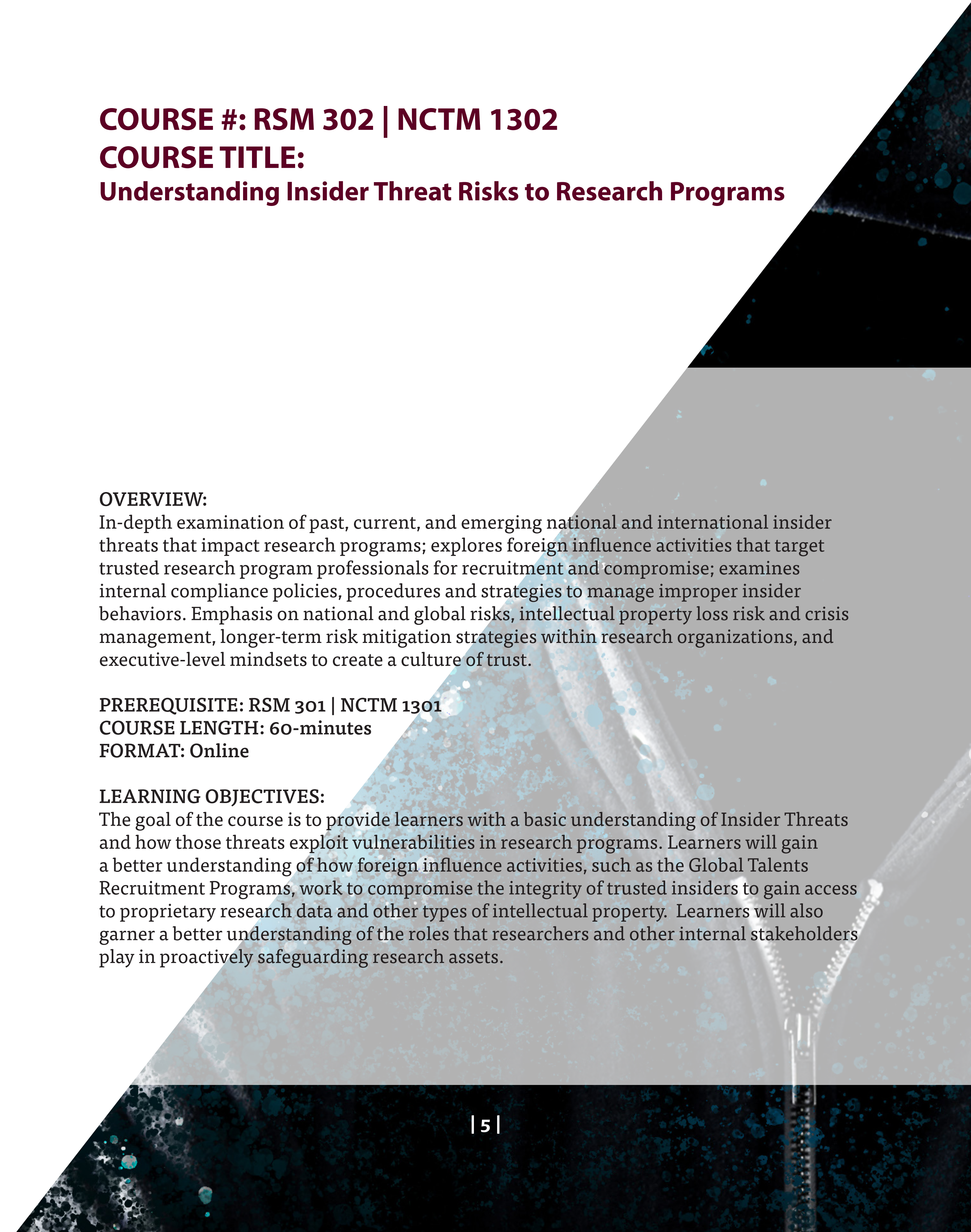
LEARNING OBJECTIVES:
The goal of the course is to provide learners with a basic understanding of the Research Security Management practice and how researchers and other internal stakeholders can participate in the proactive safeguarding of research programs. The course will provide a foundation building block for the other courses offered in the Research Security Management Certificate Program.
At the end of the course, the learner will understand Research Security Management concepts and the role that research security plays to support to all research organization stakeholders, including bench-level researchers, the executives managing research organizations, security and risk management practitioners and anyone else with an interest in safeguarding research assets.

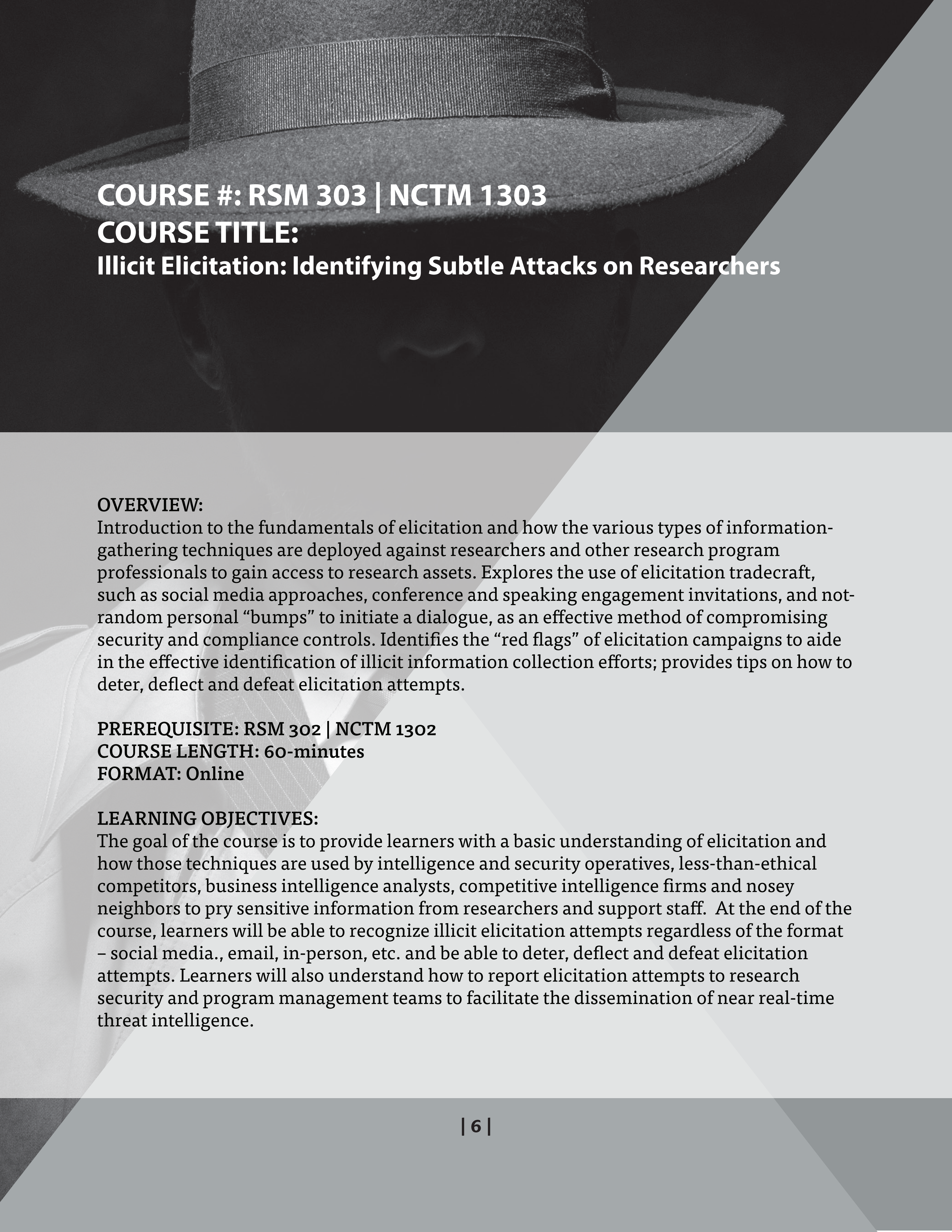
COURSE #: RSM 302 | NCTM 1302
COURSE TITLE:
Understanding Insider Threat Risks to Research Programs

OVERVIEW:
In-depth examination of past, current, and emerging national and international insider threats that impact research programs; explores foreign influence activities that target trusted research program professionals for recruitment and compromise; examines internal compliance policies, procedures and strategies to manage improper insider behaviors. Emphasis on national and global risks, intellectual property loss risk and crisis management, longer-term risk mitigation strategies within research organizations, and executive-level mindsets to create a culture of trust.

PREREQUISITE: RSM 301 | NCTM 1301
COURSE LENGTH: 60-minutes
FORMAT: Online

LEARNING OBJECTIVES:
The goal of the course is to provide learners with a basic understanding of Insider Threats and how those threats exploit vulnerabilities in research programs. Learners will gain a better understanding of how foreign influence activities, such as the Global Talents Recruitment Programs, work to compromise the integrity of trusted insiders to gain access to proprietary research data and other types of intellectual property. Learners will also garner a better understanding of the roles that researchers and other internal stakeholders play in proactively safeguarding research assets.





COURSE #: RSM 303 | NCTM 1303
COURSE TITLE:
Illicit Elicitation: Identifying Subtle Attacks on Researchers

OVERVIEW:
Introduction to the fundamentals of elicitation and how the various types of information-gathering techniques are deployed against researchers and other research program professionals to gain access to research assets. Explores the use of elicitation tradecraft, such as social media approaches, conference and speaking engagement invitations, and not-random personal "bumps" to initiate a dialogue, as an effective method of compromising security and compliance controls. Identifies the "red flags" of elicitation campaigns to aide in the effective identification of illicit information collection efforts; provides tips on how to deter, deflect and defeat elicitation attempts.

PREREQUISITE: RSM 302 | NCTM 1302
COURSE LENGTH: 60-minutes
FORMAT: Online

LEARNING OBJECTIVES:
The goal of the course is to provide learners with a basic understanding of elicitation and how those techniques are used by intelligence and security operatives, less-than-ethical competitors, business intelligence analysts, competitive intelligence firms and nosey neighbors to pry sensitive information from researchers and support staff. At the end of the course, learners will be able to recognize illicit elicitation attempts regardless of the format – social media., email, in-person, etc. and be able to deter, deflect and defeat elicitation attempts. Learners will also understand how to report elicitation attempts to research security and program management teams to facilitate the dissemination of near real-time threat intelligence.

COURSE #: RSM 304 | NCTM 1304
COURSE TITLE:
Get Off the X: Protecting Research Program Assets During Travel

OVERVIEW:
Explores the basics of protecting research assets, including research data, during travel, including domestic and international trips. Provides a summary of the common travel risks researchers face when attending poster sessions, conferences, workshops, seminars and speaking engagements. Introduces the concepts of hostile surveillance and security methods used against researchers during travel, including immigration and port-of-entry interrogations, bag and electronic device confiscations, pseudo-public transportation vulnerabilities, hotel room intrusions and personal vulnerability attacks, such “honey traps” and other blackmail techniques. Provides tips to improve the researcher’s travel security awareness and effective defensive counterintelligence techniques to better manage the risk to research program assets.

PREREQUISITE: RSM 303 | NCTM 1303
COURSE LENGTH: 60-minutes
FORMAT: Online

LEARNING OBJECTIVES:
The goal of the course is to provide learners with a basic understanding of travel security best practices that can be used to counter hostile attacks on the researcher during domestic and international travel. At the end of the course, the learner will be able to identify common techniques deployed by hostile intelligence and security agencies to target researcher vulnerabilities exposed during travel to conferences and other professional events. The learner will better understand the pre-travel countermeasure practices to adopt that initiate a travel security mindset well-before heading to the airport, including adhering to the “loaner laptop” best practice to reduce exposure of research data assets. The leaner will be able to reduce the likelihood and impact of a negative interaction with hostile officials through proper travel planning and situational awareness. The learner will also understand the need to report both overt and potential/subtle hostile encounters during travel upon his/her return to the research organization.

COURSE #: RSM 305 | NCTM 1305

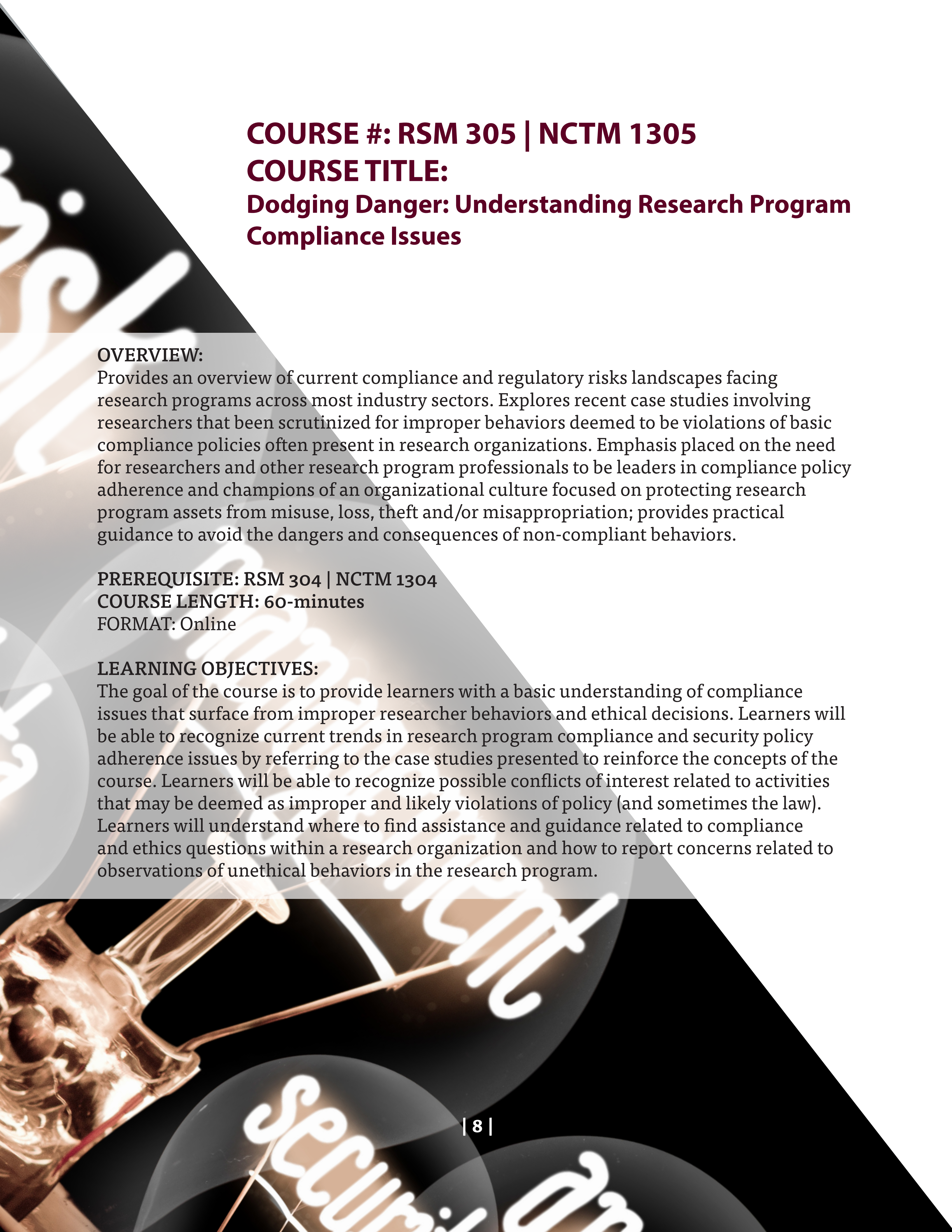
COURSE TITLE:

Dodging Danger: Understanding Research Program Compliance Issues

OVERVIEW:
Provides an overview of current compliance and regulatory risks landscapes facing research programs across most industry sectors. Explores recent case studies involving researchers that been scrutinized for improper behaviors deemed to be violations of basic compliance policies often present in research organizations. Emphasis placed on the need for researchers and other research program professionals to be leaders in compliance policy adherence and champions of an organizational culture focused on protecting research program assets from misuse, loss, theft and/or misappropriation; provides practical guidance to avoid the dangers and consequences of non-compliant behaviors.

PREREQUISITE: RSM 304 | NCTM 1304
COURSE LENGTH: 60-minutes
FORMAT: Online

LEARNING OBJECTIVES:
The goal of the course is to provide learners with a basic understanding of compliance issues that surface from improper researcher behaviors and ethical decisions. Learners will be able to recognize current trends in research program compliance and security policy adherence issues by referring to the case studies presented to reinforce the concepts of the course. Learners will be able to recognize possible conflicts of interest related to activities that may be deemed as improper and likely violations of policy (and sometimes the law). Learners will understand where to find assistance and guidance related to compliance and ethics questions within a research organization and how to report concerns related to observations of unethical behaviors in the research program.



RESEARCH SECURITY MANAGEMENT CERTIFICATE PROGRAM

THE TEXAS A&M
UNIVERSITY SYSTEM
RESEARCH SECURITY OFFICE

Presented By:

Trust Farm
SAFEGUARD INNOVATION

THE TEXAS A&M
UNIVERSITY SYSTEM
RESEARCH SECURITY OFFICE

NCTM
NATIONAL CENTER FOR
THERAPEUTICS MANUFACTURING

TEES
TEXAS A&M ENGINEERING
EXPERIMENT STATION

RESEARCH SECURITY MANAGEMENT CERTIFICATE PROGRAM

THE TEXAS A&M
UNIVERSITY SYSTEM
RESEARCH SECURITY OFFICE