APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

A Course on Understanding Insider Threat: From Threat to Risk and Trust Final Report

September 30, 2021

Steve S. Sin[1]*, Judith A. Philipson[2], Juliet R. Aiken[3], Liberty Day[1]
[1]National Consortium for the Study of Terrorism and Responses to Terrorism
[2]Advanced Research Lab for Intelligence and Security
[3]Conducere, LLC
*corresponding author, sinss@umd.edu

The Applied Research Lab for Intelligence and Security (ARLIS) is The University Affiliated Research Center (UARC) for Human Systems, Artificial Intelligence, and Information Engineering at the University of Maryland

ARLIS
7005 52nd Avenue
College Park, Maryland

EXECUTIVE SUMMARY

The National Consortium for the Study of Terrorism and Responses to Terrorism (START), Applied Research Laboratory for Intelligence and Security (ARLIS), and Conducere, LLC developed and delivered a fully online course that blends synchronous and asynchronous components on insider threat that is approximately 60 contact hours – granting 6 continuing education units (CEUs). The course included live and recorded lectures; live class discussions and activities; group in-class simulations; participation in guided online discussion forums; completion of reading materials; and participation in course evaluation processes.

Insider threat has become a common lexicon in our society today – most commonly linked with information leak and active shooter incidents. While insider threat is not a new phenomenon, there is a need for a better understanding of the phenomenon and the ways to mitigate it. This course took the form of a survey course where we examined individual, organizational, and social stressors that could contribute to insider behaviors. The course then discussed past and present trends of insider threat, response and mitigation challenges, as well as policies, procedures, and practices currently implemented (within the government and industry) to respond to and mitigate it. Finally, the course explored the systems approach to manage insider threat vis-à-vis risk assessments and risk management. In doing so, the course exposed the students to the new paradigm of thinking - shifting from insider threat to insider risk and from countering insider threat to mitigating insider risk.

By the start of course, 25 individuals had registered for the course and 63 individuals had been put on the waiting list. For the 25 individuals registered for the course, 16 individuals were U.S. students while nine were international students. For the nine international students, two were identified as being affiliated with foreign governments; three were identified as being affiliated with international organizations; three were identified as being affiliated with private industry; and one was a full-time student.

The overall impression from the post-course survey was that the course conveyed new information and that the students learned the material well, and were leaving the course with new perspectives on how to think about insider threat and how to mitigate insider threat in the future. Specifically, 100-percent of the students responding to the post-course survey strongly agreed with the statement, “I would recommend this course to my peers.” Additionally, 87.5-percent stated that they strongly agreed with the statement “overall, the course met my needs and expectations.” Finally, 87.5-percent stated that they strongly agreed with the statement, “Overall, the course increased my knowledge, skills, and abilities relevant to the course topics.”

Finally, the participants showed improvements in its knowledge on insider threat and mitigation thereof. The class average for the pre-test at the beginning of the course was 9.13 out of 15 (63.42%). The class average for the post-test, on the other hand, was 13.23 out of 15 (88.21%), showing a 24.79-percent increase in the average score and a general increase in the students’ knowledge level on topics covered during the course. Of note, all participants scored higher on their

post-tests compared to their pre-test scores. These results indicate the course contributed to student knowledge gain in the subject matter.

CONTENTS

PROJECT BACKGROUND

In line with requirements from The Defense Personnel and Security Research Center (PERSEREC), the National Consortium for the Study of Terrorism and Responses to Terrorism (START) and the Advanced Research Lab for Intelligence and Security (ARLIS), in collaboration with Conducere, LLC, developed and delivered a pilot intensive hybrid online course on understanding and countering insider threat for advanced undergraduate and graduate students as well as working professionals. The course was designed to serve as the foundational course for a future comprehensive and tailorable professionalization program developed on countering insider threat that equips the future workforce with skills to identify, assess, mitigate, and ultimately prevent the threats that insiders pose to the Department of Defense (DoD) and to national security.

The University of Maryland faculty members affiliated with START and ARLIS led the development and delivery of the pilot course, and the course involved several external (both government and private industry) guest speakers to engage with the students about various issues and considerations relevant to understanding and mitigating insider threat, vulnerabilities, consequences, and ultimately insider risk.

The pilot delivery of the course was offered to the students through the University of Maryland Office of Extended Studies from July 28 to September 22, 2021.

COURSE DESCRIPTION AND OBJECTIVES

Course Description

START, ARLIS, and Conducere, LLC produced a fully online course that blends synchronous and asynchronous course on insider threat that is approximately 60 contact hours. The course included live and recorded lectures; live class discussions and activities; group in-class simulations; participation in guided online discussion forums; completion of advance readings; and participation in course evaluation processes.

Insider threat has become a common lexicon in our society today – most commonly linked with information leak and active shooter incidents. While insider threat is not a new phenomenon, there is a need for a better understanding of the phenomenon and the ways to mitigate it. This course took the form of a survey course where the students examined individual, organizational, and social stressors that could contribute to insider behaviors. The course then discussed past and present trends of insider threat, response and mitigation challenges, as well as policies, procedures, and practices currently implemented within the U.S. Government and industry to respond to and mitigate it. Finally, the course explored the systems approach to manage insider threat vis-à-vis risk assessments. In doing so, the course exposed the students to the new paradigm of thinking - shifting from insider threat to insider risk and from countering insider threat to mitigating insider risk.

Course Objectives

The course had eight (8) terminal learning objectives designed to address PERSEREC's requirements. The eight (8) terminal learning objectives were, "After a successful completion of the course, the students will be able to":

1. Demonstrate a broad understanding of "insider threat" problem space (e.g. scope of "insider threat"; definition(s); historical trends; challenges; etc.);
2. Demonstrate a broad understanding of psychological factors that influence "insiders";
3. Demonstrate a broad understanding of environmental factors that serves to facilitate "insider threat" activities;
4. Demonstrate a broad understanding of how "insiders" exploit individual and organizational vulnerabilities to achieve their goals;
5. Critically evaluate an aspect of the "insider threat" problem space and present a coherent analysis that can inform future policy recommendations;
6. Look at complex ("insider threat") questions and identify how it impacts and is impacted by political, social, economic, legal, and/or ethical dimensions;
7. Critically evaluate and recommend for implementation vulnerability reduction measures to reduce overall risk due to insiders; and,
8. Communicate scientific and policy ideas – as well as the risks associated with some scientific and policy ideas – effectively through a written report, and oral participation in class.

COURSE DESIGN AND CONTENT

Course Design

To maximize learning outcomes by accommodating different learning styles while simultaneously providing an opportunity for a larger student pool to take the course (not to mention to mitigate the increased uncertainty presented by the COVID-19 pandemic), we designed a fully online course that includes both synchronous and asynchronous components. Cognizant that the potential student population would include working professionals, the synchronous component of the course met twice per week for a total of 180 minutes (90 minutes per meeting) over the 10-week course period on Tuesdays and Wednesdays from 11:30 AM to 1:00 PM U.S. Eastern Time. Tuesdays and Wednesdays were chosen as the days to hold synchronous class meetings as they avoided the beginning and end of the week demands the students might have from their full time positions or other schoolwork. Likewise, 11:30 AM to 1:00 PM U.S. Eastern Time was chosen to accommodate students from all U.S. time zones as well as those from Europe and Australia. In terms of course activities, the synchronous portion of the course included live lectures, class discussions, group activities, external guest speakers, and simulation exercises.

Through the use of asynchronous delivery, the course was able to cover additional substantive materials as well as further engage with the students. The course was able to accomplish this by providing students with pre-recorded lectures, pre-recorded guest speaker presentations, and facilitated post-reading discussion posts. Although the asynchronous portion of the course is designed to be somewhat self-paced, the students were required to follow an overall course

schedule as noted in the course syllabus to ensure they are prepared for the synchronous portions of the course as well as to complete all required work on time.

Overall, the course was designed for the students to spend between one to two hours per day (on average) on course work between 28 July and 22 September 2021. See Appendix A1, Course Syllabus, for a detailed description of course completion requirements and course schedule.

"Understanding the psychology behind insider threat allows me to make the Insider Threat program into a positive program that can enhance EP programs while providing organizations better options to mitigate insider threat"

– Participant Comment

Course Content

The course included four distinct yet interconnected modules. Module 1 discussed the individual and environmental factors and stressors that could facilitate or amplify insider threat behavior through the lens of industrial and organizational psychology. In this module, students were pushed to consider and explore the bounds of the term "insider threat" as well as how an individual or individuals could become an "insider threat" either through their own volition or because of circumstances. Students also explored how an organization could proactively prevent and mitigate formation of "insider threat" through adoption of better working environment, clearer and more equitable policies, as well as improved constructive organizational culture. The content for this module was delivered through recorded lectures, reading materials, synchronous class discussions and activities, and facilitated asynchronous discussions.

Module 2 discussed how one can improve threat assessment by understanding the decision-making science. The module aimed to develop critical thinking skills to improve students' competencies in threat detection and risk management. In this module, students were exposed to various situations where they have to determine how a malicious actor was able to deceive others. Students were also presented with situations where they have to determine the presence of deception in a guest speaker. To accomplish this, this module was specifically designed to leverage different learning styles through a mix of live synchronous lectures, large and small group discussions, viewing of video clips, listening to audio clips, creative writing assignments, and participation of external guest speakers.

"Good comprehensive course, with much interaction between participants, extensive readings about subjects, and enthusiastic teaching modes [instructors' passion about the subject matter]."

– Participant Comment

Module 3 discussed adopting risk management approach to mitigating insider threat. The module introduced the students to systematic risk assessment processes and forced the students to think beyond personnel vetting as the method of personnel risk management in mitigating insider threat. The module emphasized to the students that "threat" is only one part of the equation for risk, and that adoption of a risk management approach to mitigate insider threat really means *managing insider risk* – through a holistic examination of vulnerabilities, consequences, as well as threat. Finally, the module discussed the challenges associated with the

risk management approach by explicating the different perspectives of people involved in the risk assessment and management process in an organization. The content for this module was delivered through recorded lectures, recorded guest speaker presentations, and facilitated asynchronous discussions.[1]

Finally, Module 4 was the capstone exercise for the course, consisting of a series of scenario-driven synchronous online simulations. The capstone exercise was designed to bring everything that the students have learned throughout the course together by having the students "play" various roles in a company that has to respond to a potential insider threat incident. The students were first presented with a vague potential insider threat that may or may not be present in the fictitious corporation where they are all a member. The Chief Executive Officer (CEO) of the fictitious corporation (played by Dr. Steve Sin, the lead instructor) directed the leadership team (the students) to discuss the potential situation and recommend some courses of action. The students were then presented with several new policies that the CEO would like them to implement. At this juncture, the students discussed the pros and cons of each policy measure as well as their potential effectiveness. Finally, the students were presented with several potential suspicious cases that were detected after the implementation of these new policies. Upon presentation of these cases, students had to decide which case presents the highest risk to the organization and why. For the duration of the exercise, each student was assigned a specific role within the company (e.g., human resources, lead engineer, security, etc.) and they had to make their recommendations and determinations from the perspective of the personnel that is working in that function for the organization. The goal of the capstone exercise was for the students to understand the challenges of adopting insider threat (or insider risk) mitigation framework for an organization that will adequately mitigate both seen and unseen threats while maintaining the positive organizational culture and reducing overall risk.

See Appendix A2, Course Reading List, for a list of reading materials for the course.

Guest Speakers

The course invited several external speakers to present and discuss with the students on various topics relevant to insider threat and risk. First, on the topic of deception detection, an individual who is information operations expert and consultant in the field demonstrated to the students in real time how easy it was to fool someone by framing the messages and communications students were shown, in real time, how easy it is to fool someone by framing the messages and selected communications methods. Next, a panel discussion from four senior practitioners of a federal government insider threat center discussed how the behavioral sciences, law enforcement, threat management, and counterintelligence work together to assess potential threats. Additionally, a former career intelligence officer and author, discussed the role of cultural intelligence and its application to insider threat detection and risk management. Finally, a practitioner from private

[1] Module 3 was originally designed to have synchronous lectures, class activities, and guest speaker, but we changed the module to asynchronous delivery to accommodate students' religious observances.

industry discussed the advantages of moving from insider threat to insider risk through adoption of risk management approaches as well as its associated challenges.

STUDENT RECRUITMENT

Undergraduate/Graduate Credit Granting Course

As PERSEREC's intent was to ultimately develop a program targeting primarily advanced undergraduate students, graduate students, and young professionals, we sought to gain university administrative approval for a 3-credit summer course with an undergraduate section and a graduate section, to be delivered during the summer session of 2021. To do this, START's Program Director for Education and Training, Ms. Liberty Day, consulted with the Associate Dean for Research and Graduate Studies for the College of Behavioral & Social Sciences to add the course onto the University of Maryland's Student Information System (SIS). Once she received permission to add the course onto the SIS, she then worked with the Office of Extended Studies (OES), the University of Maryland entity that administers summer courses, to confirm the nonstandard course dates (as the course was designed to run for 10 weeks, two weeks longer than the usual summer courses), input instructor information into the budgets and contracts system, and manage all instructor contracting requirements. These steps ensured that the course was listed and resourced to receive student registrations.

To recruit prospective students to take the course, Ms. Day coordinated with various Directors of Undergraduate Studies (DUGS) and Directors of Graduate Studies (DGS) throughout the university as well as START's communication manager and the course instructors to actively promote the course through a variety of channels. Channels utilized to promote the course included START's newsletter, START's social media accounts, individual marketing emails, various university listservs, and various DOD listservs (including the PERSEREC Threat Lab listserv). Despite active marketing and promotion of the course for several months, only 2 students registered for the course – both current University of Maryland students. There were some working professionals who were interested in taking the course, but the cost of the course was prohibitive for the working professional to take the course without some sort of subsidy to defray the registration cost.

Approximately three weeks prior to the start of the class, Ms. Day, in coordination with the instructors, ARLIS, and the sponsor, cancelled the course and withdrew it from the course listings due to the low enrollment.

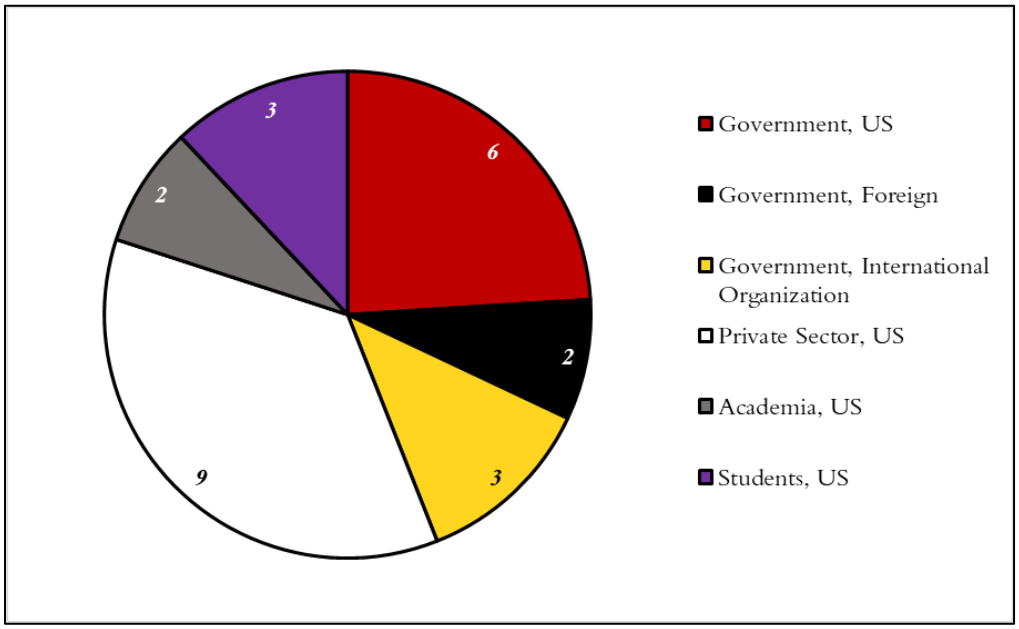
Open Learning Continuing Education Unit Granting Course

Given that the course did not draw enough interest as a course for advanced undergraduate and graduate students, START and ARLIS, in coordination with the sponsor, decided to convert the course into an open learning course that grants Continuing Education Units (CEUs), targeting working professionals. (See Appendix A1 for the CEU course syllabus; Appendices A3, A4, and A5 for the course application documents filed with the OES to establish the course in the system). Ms. Day again worked with OES to ensure the course is properly approved by the university and listed on the course catalog.

To market the course, Ms. Day worked with START's communications manager to develop a marketing plan and to set up an early registration process. The course was primarily promoted through START's newsletter and social medial accounts. The course was also promoted through a few listservs and personal contact lists. Unlike the undergraduate/graduate course, within 72 hours of initiating the marketing efforts, over 100 people contacted Ms. Day with an interest to register for the course.

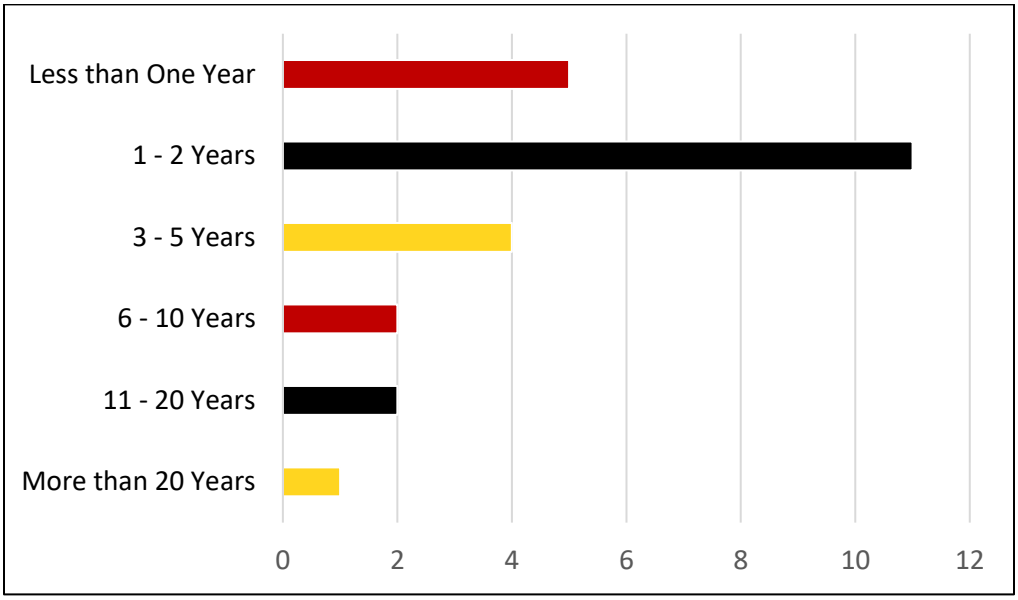
By the start of course, 25 individuals had registered for the course and 63 individuals had been put on the waiting list. For the 25 individuals registered for the course, 16 individuals were U.S. students while nine were international students. For the nine international students, two were identified as being affiliated with foreign governments; three were identified as being affiliated with international organizations; three were identified as being affiliated with private industry; and one was a full-time student. For the two students who were identified as being affiliated with the foreign government, one student was affiliated with the Royal Canadian Mounted Police while the other student was affiliated with the Turkish Army. For the three students who were identified as being affiliated with international organizations, two were affiliated with the United Nations while one was affiliated with the Organization of American States. ***Figure 1***, below, provides a detailed breakdown of students enrolled in the course by category:

Figure 1: Course Enrollment Student Breakdown by Category



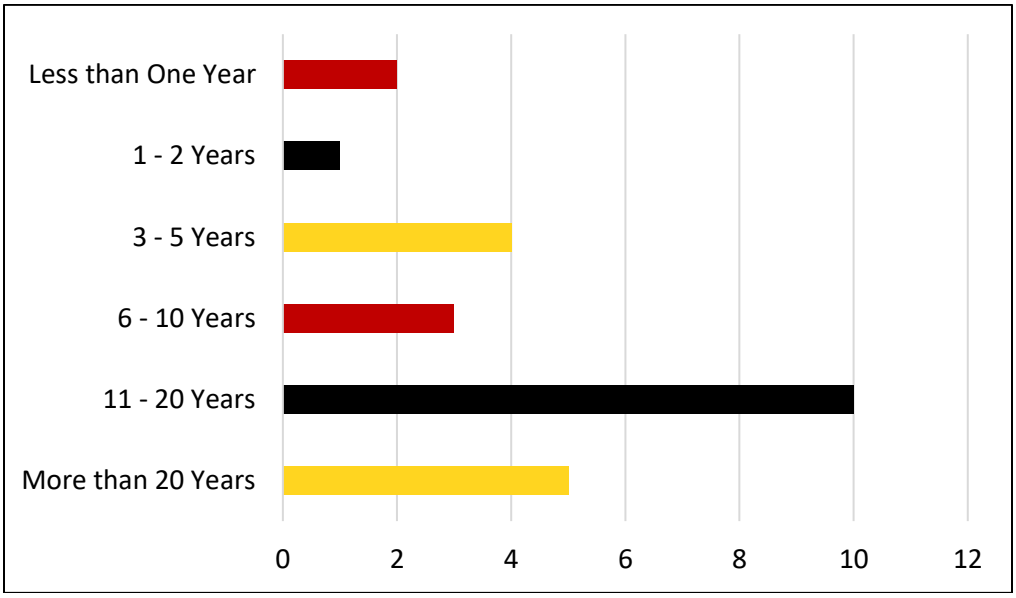
For the 25 students who registered for the course, majority of the students had been in their current positions for five years or less. Of that group, most had been in their positions between one and two years. **Figure 2**, below, provides an illustration of the student body categorized by the length of time in their current positions.

Figure 2: Student Body Length of Time in Current Position



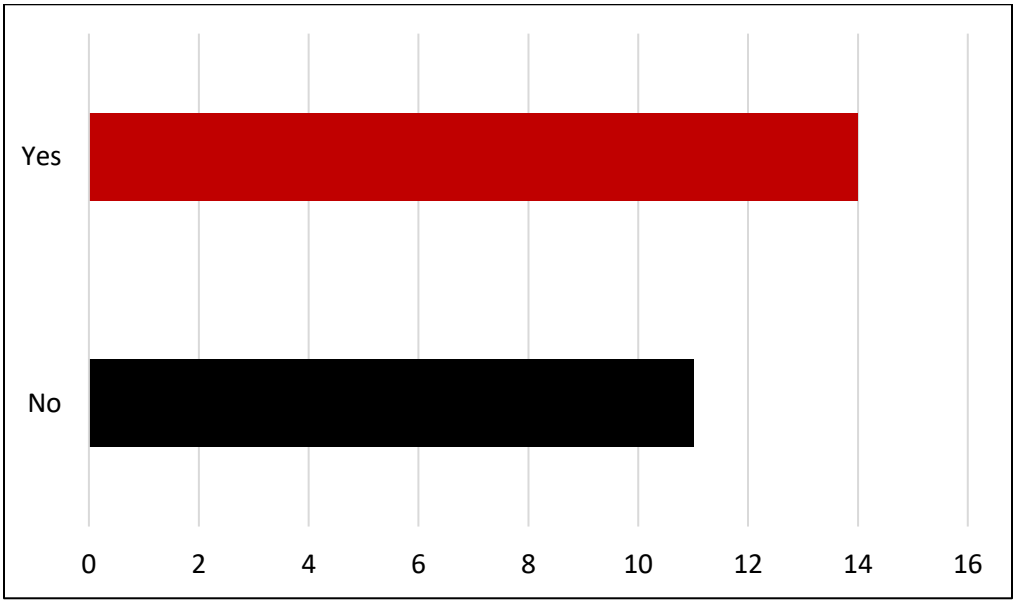
Although the majority of the student body had been in its current position for five years or less, the majority of the student body were mid- to late-career professionals. **Figure 3**, below, provides an illustration of the students' length of time in their respective professions:

Figure 3: Student Body Length of Time in the Profession



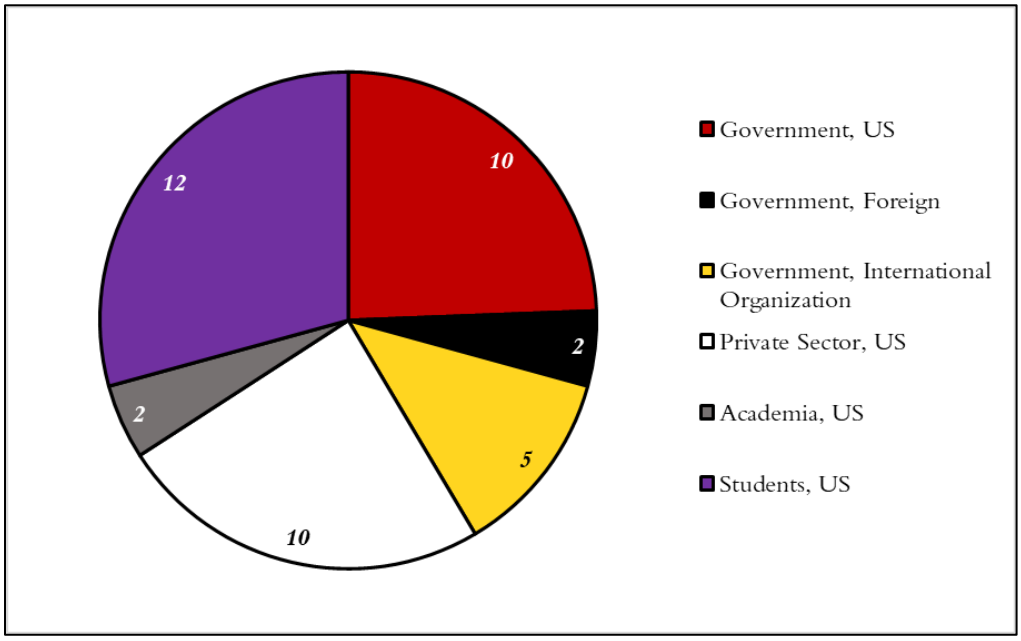
Additionally, while all students were working in insider threat relevant positions, 44-percent of the students worked in positions that did not directly deal with identifying or mitigating insider threat. **Figure 4**, below, provides an illustration of the student body breakdown:

Figure 4: Students Currently Working in Positions Directly related to Insider Threat Detection/Mitigation



For the 63 individuals who were waitlisted for the course, we were able to identify 21 as being from the U.S. while 19 were identified as international students. We were not able to identify the enrollment locations or the nationality of 23 individuals on the waiting list. **Figure 5**, below, provides a detailed breakdown of individuals waitlisted for the course by category:

Figure 5: Course Waiting List Breakdown by Category



A survey of those waitlisted revealed that the overwhelming majority of them would like to take the course if it were to be offered again in the future.

COURSE CONDUCT

Overall, the course delivery was smooth and occurred without any issues. Throughout the conduct of the course, Mr. William Stephens, Director of Counterintelligence Research and Professor of Practice, of ARLIS/University of Maryland joined the classes and provided unique experiences and perspectives on the subjects being discussed in class. His involvement in the conduct of the classes enriched the course content during class discussions and group activities. Mr. Stephens was an invaluable addition to the course that occurred organically during the conduct of the course rather than something that was planned during the design and development phase of the course.

The student body was especially eclectic and interesting – ranging from one to two years to over twenty years of experience working in insider threat relevant positions. The diverse range of experiences as well as the types of organizations the students were affiliated with made for very interesting class discussions with varied perspectives on the subjects being discussed.

A challenging part of the student body was that only about 50% of the students attended the classes at any given time. After approximately five class sessions, the class attendance "stabilized" to 14 dedicated students who would always attend and submit all assignments. The remainder of the students either stopped showing up to class or formally withdrew– we had three students who formally withdrew, citing work schedule conflicts. Although class attrition was expected given the make-up of the student body, the attrition rate (44-percent) was higher than we had originally anticipated – we had originally anticipated between 20- to 32-percent attrition rate (5 to 8 students) based on other University of Maryland open learning courses targeting working professionals. The attrition rate for the course, however, was on par with or better than other open learning courses with long course durations (none of which require as many synchronous participations as this course) and are offered for free.

We believe two primary factors affected the course's completion rate. First, the student body was made up of working professionals and committing to attending synchronous classes over a 10-week period consistently could be difficult due to changing work commitment. Second, the course was not a required course. In other words, other than the incentive of receiving six CEUs at the end of the course, there was not an added incentive for the students to complete the course – such as the students' employers requiring them to complete the course, students had to pay for registration fee out of pocket, etc.

"I thoroughly enjoyed this class. The diversity of course instructors was a strong point. By far and away, the most advantageous aspect was the range of students in the course."
– Participant Comment

Options for Future Delivery

Given the number of students waitlisted and responses from those waitlisted, there certainly was a demand for future iterations of the course. At the moment, there are three potential avenues to deliver additional iterations of this course. First, the course has been approved through the University of Maryland's OES for one calendar year; thus, we can deliver this course again at any time until mid-July 2022. This would be the easiest method to offer additional iterations of this course. Additionally, if the course continues to generate interest, then an extension/renewal for course approval could be filed so that the course could be delivered beyond the current approval date. As the course was offered free of charge to those who sign up, and if the course is to be offered for free in the future, additional funding would be required to deliver any future iterations of the course.

Another option is to continue to offer this course in the future using the OES structure as we have done with the pilot course but charge the students a fee to cover some of the costs of running the course. There most likely still will be a need for some funding support to cover the delivery cost, but the amount of additional funding needed could be smaller depending on how much registration fee each student will be charged to register for the course. Of course, this could have an impact on the number of students interested in signing up for the course. On the other hand, charging for the course could provide an incentive for those students who sign up to complete the course, thus decreasing the attrition rate for the course.

Finally, the course could be incorporated into the University of Maryland's Master of Professional Studies (MPS) in Security and Terrorism Studies program, which is a fully online graduate degree that is being administered by START. While this option may require less amount of funding up front, additional funding would still be required for the administrative and development tasks of converting the course into a fully accredited graduate course. Once the course has been developed and approved by the University of Maryland, no additional funding would be required to deliver the course since the delivery costs would be covered by student tuition. The primary barrier for this option, perhaps, is the fact that working professionals who would like to take the course would have to pay the graduate tuition associated with the course, which would be significantly higher than the professional training course being offered through OES (even if we started charging for the open learning OES course).

COURSE OUTCOMES/EVALUATIONS

To evaluate learning outcomes for the course, the course had two built-in evaluation metrics that corresponded to levels 1 and 2 of Kirkpatrick's training evaluation[2]. Kirkpatrick's model for learning evaluation is the most well-known and widely used model to analyze training and education program outcomes. The strength of the model is that it can be applied to any style of training/education – both formal and informal – to determine the aptitude based on four level criteria. Level 1 of the evaluation is "reaction," where it measures how the participants reacted/felt about the training (e.g., course satisfaction survey). Level 2 is "learning," where it measures how much the participants gained/retained the knowledge after the training/education. Ordinarily, this level is measured through the administration of pre- and post-course tests and comparing the outcomes of those tests. Level 3 is "behavior," where it measures how the participants are utilizing what they have learned at their daily work after they have completed the training/education program. Ordinarily, this measurement would be done through a post-course survey sent to the participants approximately six- to 12-months after the completion of the training/education program. Finally, Level 4 is "Results," where it measures whether the training/education program had a positive impact on the organization where the participants work. This level of measurement would ordinarily be measured through a post-course survey sent to the organizations where the participants work approximately 12- to 18-months after the completion of the training/education program.

> "Overall, I liked how the class was run. I took DIA's week-long analyst course, and I think this class could be a follow up course to that. The DIA analyst course made you familiar with identifying certain elements to look for and how to respond appropriately. This course got into the why behind what motivates people and what affects our biases as analysts."
>
> *– Participant Comment*

Given that it was impractical for the research team to obtain levels 3 and 4 assessments for the course, we decided to implement levels 1 and 2 of the Kirkpatrick's evaluation model for the course. First evaluation metric was the post-course survey to gain subjective impressions from the students about the learning that occurred during the class. This metric satisfied Kirkpatrick's level 1 training evaluation. The second evaluation metric was the pre- and post-tests. All students were administered a pre-test on the first day of class before any course materials were presented to them. At the end of the course, the students were administered a post-test to gauge whether there had been any change in the overall level of student knowledge in the subject after taking the course. This metric satisfied Kirkpatrick's level 2 training evaluation.

> "I will incorporate professional security measures in my work to guard against insider threats"
>
> *– Participant Comment from Post-Course Survey*

The overall impression from the post-course survey was that the course conveyed new information and that the students learned the material well, and were leaving the

[2] Kirkpatrick, J. D., & Kirkpatrick, W. K. (2016). Kirkpatrick's four levels of training evaluation. Association for Talent Development.

course with new perspectives on how to think about insider threat and how to mitigate insider threat in the future. Specifically, 100-percent of the students responding to the post-course survey strongly agreed with the statement, "I would recommend this course to my peers." (See **Figure 6** below). Additionally, 87.50-percent stated that they strongly agreed with the statement "overall, the course met my needs and expectations." (See **Figure 7** below). Finally, 87.50-percent stated that they strongly agreed with the statement, "Overall, the course increased my knowledge, skills, and abilities relevant to the course topics." (See **Figure 8** below).

Also see Appendix A-6, Post-Course Survey Questions and Results, for all post-course survey responses.

Figure 6: I would Recommend This Course to My Peers (Post-Course Survey Results)

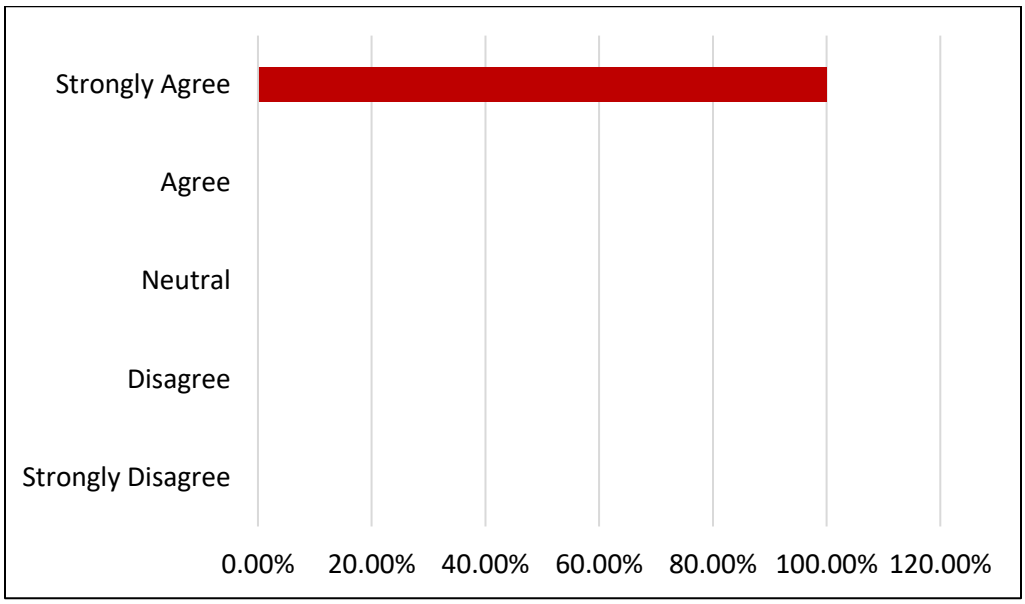


Figure 7: Overall, The Course met My Needs and Expectations (Post-Course Survey Results)

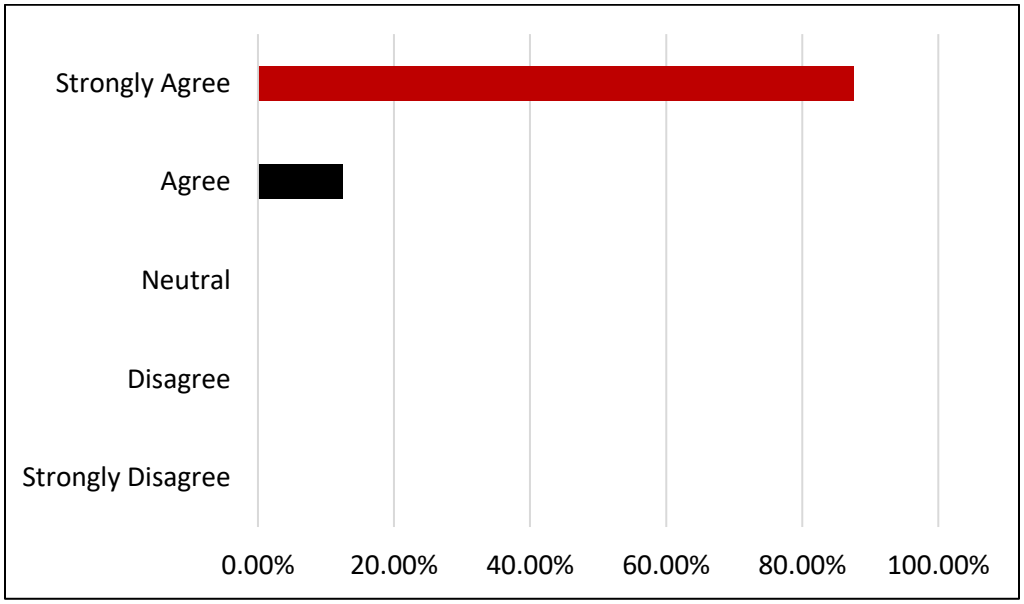
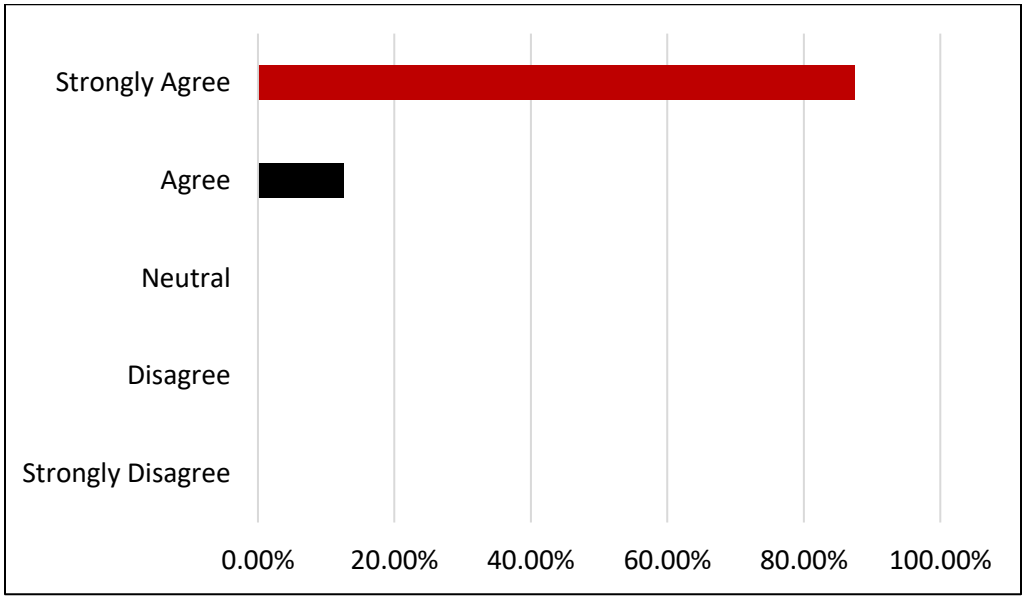


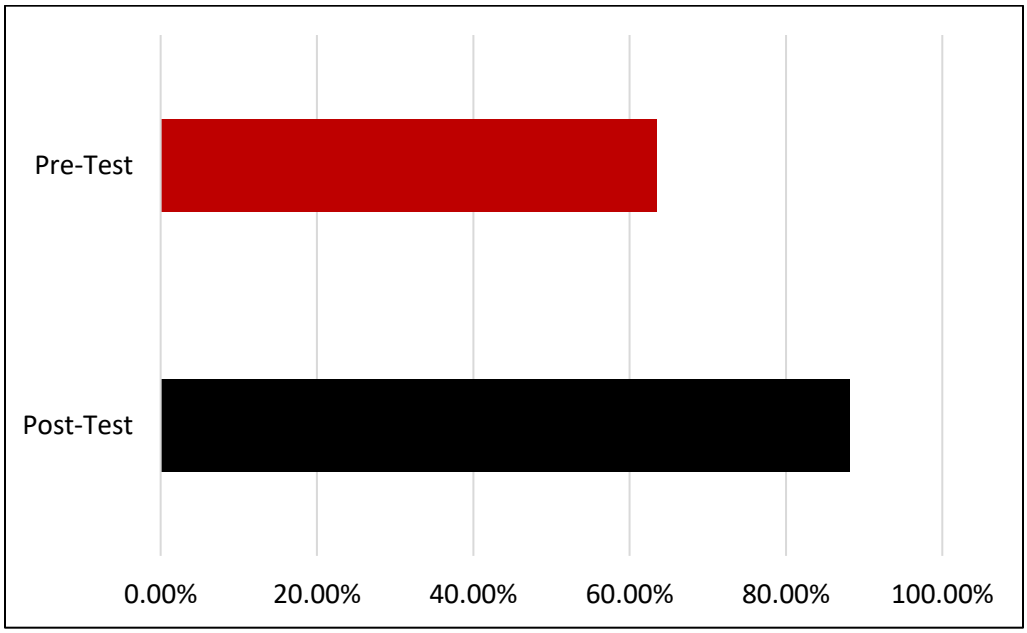
Figure 8: Overall, the course increased my knowledge, skills, and abilities relevant to the course topics (Post-Course Survey Results)



Additionally, the class showed improvements in its knowledge on insider threat and mitigation thereof. The class average for the pre-test, administer at the beginning of the course, was 9.13 out of 15 (63.42%). The class average for the post-test, on the other hand, was 13.23 out of 15 (88.21%), showing a 24.79-percent increase in the average score and a general increase in the students' knowledge level on the topics covered by the course. Of note, all students scored higher on the post-test when compared to their pre-test scores.

These results indicate the course contributed to student knowledge gain in the subject, as measured utilizing both Kirkpatrick's level 1 (post-course surveys) and level 2 (pre-/post-test) training evaluation methods. **Figure 9**, below, provides an illustration of the class averages for the pre- and post-test for the course.

Figure 9: Pre- and Post-Test Class Averages



LESSONS LEARNED

There were two major lessons learned from the development and delivery of the course worth noting. First, insider threat and the topic of insider threat is not something that resonates with undergraduate and graduate students outside of a very specific context. Some students might be aware of the term, and some might be interested in learning more about the phenomenon, but those students tend to be in informatics, cybersecurity, or security studies related disciplines – in other words, the subject matter is not something that resonates with a wide population of the university's student body. Thus, offering an insider threat course as a summer course outside of these specific contexts resulted in low enrollment and interest for the course. Given this, if PERSEREC desires to develop a program aimed at the undergraduate and graduate population, the program must be situated within a larger program of a discipline (such as security studies, cybersecurity, etc.) where its student body already has some interest and awareness about the insider threat issues for it to gain traction with undergraduate and graduate students.

Second, if the course will remain as a professional training/development course for working professionals, formatting future courses as facilitated asynchronous course may allow for even higher interest and enrollment due to the flexibility that an asynchronous course provides. Since a facilitated asynchronous course will largely be a self-paced course and the students could devote

time to work on the coursework outside of their regular work hours, a facilitated asynchronous course may also serve to increase the course completion rate. One thing we would have to be cognizant of with this option is that we would need to re-imagine the course evaluation criteria to ensure the quality of learning outcome is maintained. Finally, the course would lose what turned out to be its biggest strengths – insights students gained by interacting with each other, with the instructors, and guest speakers (as pointed out by the students – if we were to deliver this course in an asynchronous manner.

ACKNOWLEDGEMENTS

This report was prepared for [Office of the Undersecretary of Defense for Intelligence and Security (OUSD(I&S)), United States Department of Defense (DoD)] under the following agreement:

HQ003420F0655, *University of Maryland,* "Insider Threat and Personnel Vetting."

DISCLAIMERS

Any views, opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of an official United States government position, policy, or decision. Additionally, neither the United States government nor any of its employees make any warranty, expressed or implied, nor assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process included in this publication.

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the Applied Research Laboratory for Intelligence and Security (ARLIS), the University of Maryland, or the United States government, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

ABOUT ARLIS

Applied Research Laboratory for Intelligence and Security (ARLIS) is a UARC based at the University of Maryland College Park and established in 2018 under the auspices of the OUSD(I&S). ARLIS is intended as a long-term strategic asset for research and development in artificial intelligence, information engineering, acquisition security, and social systems. One of only 14 designated United States Department of Defense (DoD) UARCs in the nation, ARLIS conducts both classified and unclassified research spanning from basic to applied system development and works to serve the U.S. Government as an independent and objective trusted agent.

Technical Points of Contact:

PI: Adam Russell, D.Phil.
Chief Scientist, ARLIS
301.226.8834; arussell@arlis.umd.edu

Co-PI: Kelly Jones, Ph.D.
Assistant Research Scientist, ARLIS
301.226.8850; kjones@arlis.umd.edu

Task Lead: Steve Sin, Ph.D.
Director, Unconventional Weapons and Technology Division, START, UMD
301.405.6656; sinss@umd.edu

Task Lead: Judy Philipson, Ph.D.
Associate Research Scientist, ARLIS
202.257.5859; jphilipson@arlis.umd.edu

Administrative Points of Contact:

Ms. Monique Anderson
Contract Officer, Office of Research Administration
Assistant Director, ARLIS
301.405.6272; manders1@umd.edu

APPENDICES

A.1: Course Syllabus

Understanding Insider Threat: From Threat to Risk and Trust

July 28 – September 22, 2021

Online Course Syllabus

Instructors:

Steve Sin, Ph.D.
(sinss@umd.edu)
Assistant Research Scientist & Director, Unconventional Weapons and Technology Division
National Consortium for the Study of Terrorism and Responses to Terrorism
University of Maryland

Judy Philipson, Ph.D.
(jphilipson@arlis.umd.edu)
Associate Research Scientist, Applied Research Lab for Intelligence and Security
University of Maryland

Juliet Aiken, Ph.D.
(jaiken@conducerellc.com)
Co-Founder and Chief Consulting Officer, Conducere, LLC

Course Description:

The National Consortium for the Study of Terrorism and Responses to Terrorism (START), Applied Research Laboratory for Intelligence and Security (ARLIS), and Conducere, LLC produced a fully online course that blends synchronous and asynchronous course on insider threat that is approximately 60 contact hours. The course includes live and recorded lectures; live class discussions and activities; group in-class simulations; participation in guided online discussion forums; completion of advance readings; and participation in course evaluation processes.

Insider threat has become a common lexicon in our society today – most commonly linked with information leak and active shooter incidents. While insider threat is not a new phenomenon, there is a need for a better understanding of the phenomenon and the ways to mitigate it. This course will take the form of a survey course where we examine individual, organizational, and social stressors that could contribute to insider behaviors. The course will then discuss past and present trends of insider threat, response and mitigation challenges, as well as policies, procedures, and practices currently implemented within the U.S. Government to respond to and mitigate it. Finally, the course will explore the systems approach to manage insider threat vis-à-vis risk assessments. In doing so, the course will expose the participants to the new paradigm of thinking - shifting from insider threat to insider risk and from countering insider threat to mitigating insider risk.

Prerequisites:

There are no pre-requisites for this course.

Terminal Learning Objectives:

After completing this training, you will be able to:

- Demonstrate a broad understanding of "insider threat" problem space (e.g. scope of "insider threat"; definition(s); historical trends; challenges; etc.);
- Demonstrate a broad understanding of psychological factors that influence "insiders";
- Demonstrate a broad understanding of environmental factors that serves to facilitate "insider threat" activities;
- Demonstrate a broad understanding of how "insiders" exploit individual and organizational vulnerabilities to achieve their goals;
- Critically evaluate an aspect of the "insider threat" problem space and present a coherent analysis that can inform future policy recommendations;
- Look at complex ("insider threat") questions and identify how it impacts and is impacted by political, social, economic, legal, and/or ethical dimensions;
- Critically evaluate and recommend for implementation vulnerability reduction measures to reduce overall risk due to insiders; and,
- Communicate scientific and policy ideas – as well as the risks associated with some scientific and policy ideas – effectively through a written report, and oral participation in class.

Course Schedule:

This is a synchronous and asynchronous facilitated course. The course will begin with a synchronous class meeting on Wednesday, 28 July 2021, from 11:30 AM to 1:00 PM Eastern Time. While the asynchronous portion of the course is self-paced and you can work on those course materials at any time after 28 July, the synchronous portion of the course will meet twice per week – from 11:30 AM to 1:00 PM Eastern Time on Tuesdays and Wednesdays – throughout the duration of the course. Although the asynchronous portion of the course is self-paced, the course will follow an overall schedule and the instructors will provide you with additional instructions during the synchronous portion of the course. To stay on schedule, you can expect to spend between 1-2 hours per day (on average) between 28 July and 22 September 2021 on course work.

You must complete modules and lessons in sequential order. All modules, lessons, discussion posts, etc. will remain locked until you complete previous course components, or the release date of the material has been met.

Class Date (MM/DD)	Recommended Completion Date (MM/DD)	Course Activities / Assignment	Contact Time
07/28	07/28	**Class Activity (Synchronous):** Introduction to Insider Threat	90 minutes
		Assignments (Asynchronous):	
	07/29	1. Pre-test	25 minutes
	08/02	2. Advance Reading	150 minutes

	08/02	3. View Recorded Lecture for: "The 'I' (Individual) in Insider Threat"	45 minutes
08/03		**Class Activity (Synchronous):**	
	08/03	Class discussion and activities	90 minutes
		Assignments (Asynchronous):	
	08/03	1. Advance Reading	150 minutes
	08/03	2. Discussion Post #1	30 minutes
08/04		**Class Activity (Synchronous):**	
	08/04	Class discussion and activities	90 minutes
		Assignments (Asynchronous):	
	08/09	1. Advance Reading	150 minutes
	08/09	2. View Recorded Lecture for: "The 'E' (Environment) in Insider Threat"	45 minutes
08/10		**Class Activity (Synchronous):**	
	08/10	Class discussion and activities	90 minutes
		Assignments (Asynchronous):	
	08/10	1. Advance Reading	150 minutes
	08/10	2. Discussion Post #2	30 minutes
08/11		**Class Activity (Synchronous):**	
	08/11	Class discussion and activities	90 minutes
		Assignment (Asynchronous):	
	08/16	1. Advance Reading	180 minutes
08/17		**Class Activity (Synchronous):**	
	08/17	In-person Lecture: Why We are So Easily Fooled – Social Engineering and the Malicious Insider	90 minutes
		Assignments (Asynchronous):	
	08/17	1. Advance Reading	180 minutes
	08/17	2. Discussion Post #3	30 minutes
08/18		**Class Activity (Synchronous):**	
	08/18	Class discussion and activities	90 minutes
		Assignment (Asynchronous):	
	08/23	1. Advance Reading	150 minutes
08/24		**Class Activity (Synchronous):**	

	08/24 08/25	Class discussion and activities **Assignment (Asynchronous):** 1. Advance Reading	90 minutes 180 minutes
08/25	 08/25 08/30 08/30	**Class Activity (Synchronous):** In-person Lecture: Making Better Decisions – Identifying and Reporting Threats and Assessing Risk **Assignments (Asynchronous):** 1. Advance Reading 2. Discussion Post #4	 90 minutes 180 minutes 30 minutes
08/31	 08/31 09/01	**Class Activity (Synchronous):** Class discussion and activities **Assignment (Asynchronous):** 1. Advance Reading	 90 minutes 150 minutes
09/01	 09/01 09/07 09/07	**Class Activity (Synchronous):** Class discussion and activities **Assignments (Asynchronous):** 1. Advance Reading 2. Discussion Post #5	 90 minutes 150 minutes 30 minutes
09/07	 09/07 09/07	**Class Activity (Asynchronous):** Lecture: Risk Management Approach to Address Insider Threat **Assignment (Asynchronous):** 1. Read Capstone Exercise Rules and Role Sheet	 30 minutes 60 minutes
09/08	 09/08 09/14	**Class Activity (Asynchronous):** 1. Capstone Exercise Introduction and Instructions **Assignment (Asynchronous):** 1. Read Capstone Exercise Rules and Role Sheet	 30 minutes 60 minutes
09/14	 09/14	**Class Activity (Synchronous):** Capstone Exercise Scenario 1	 90 minutes
09/15		**Class Activity (Synchronous):**	

	09/15 09/15	1. Capstone Exercise Scenario 1 Discussion 2. Capstone Exercise Scenario 2	15 minutes 75 minutes
09/21	 09/21	**Class Activity (Synchronous):** 1. Capstone Exercise Scenario 2 2. Capstone Exercise Scenario 2 Discussion 3. Capstone Exercise Scenario 3	 30 minutes 15 minutes 45 minutes
09/22	 09/22 09/22 09/22 09/22 09/22	**Class Activity (Synchronous):** 1. Capstone Exercise Scenario 3 2. Capstone Exercise Scenario 3 Discussion 3. Capstone Exercise AAR **Assignments (Asynchronous):** 1. Post Test 2. Satisfaction Survey	 45 minutes 15 minutes 30 minutes 25 minutes 10 minutes
		Total Contact Time	**3,600 minutes (60 hours)**

Course Completion Requirements:

In order to complete the course, you will need to finish an ungraded pre-test and post-test, and an ungraded satisfaction survey. In addition, you will be required to participate in a minimum of four (4) discussion posts throughout the course, attendance of a minimum of nine (9) synchronous meetings, and participation in **ALL** of the virtual synchronous Capstone Exercise (scheduled at the end of the course). Successful course completion will be determined by meeting the requirements outlined above as well as achieving a cumulative score of at least 70%. Your final grade will consist of the following:

- Discussion Posts: 20 total points (5 points per post)
- Attendance of Synchronous Class Sessions: 45 total points (5 points per session)
- Capstone Exercise: 35 points

Discussion Posts:

Your participation in four (4) discussion posts will be will collectively contribute to 20% of your overall grade. Your posts will be assessed for topic relevance, communication of ideas, and demonstration of critical thinking. Each discussion board post will contribute to 5% of your overall grade.

Synchronous Session Attendance (and participation):

As this course includes quite a number of in-class activities and discussions, class attendance and participation are essential in order for everyone to have a positive experience with the course. As such, Synchronous Session Attendance (and participation) will consist of: 45% of your overall grade. The participants will be given a class attendance/participation "grade" of *check-plus, check*, or *check-minus* for each synchronous session. At the end of the course, the *check-pluses*, *checks*, and *check-minuses* will be totaled to arrive at each participant's attendance/participation grade. Throughout the course, there are 13 synchronous class sessions not counting the synchronous Capstone Exercise sessions. Of these 13 synchronous class sessions, a participant must attend a minimum of nine (9) sessions (essentially, each participant receives up to four (4) penalty-free absences between these dates). For each "graded" session, participants can earn up to 5% of the overall grade. Full 5% will be given to the participants with *check-pluses* for the session. Participants with *checks* will receive 4% for the session. Participants with *check-minuses* will receive 2% for the session.

To earn a *check-plus*, a participant must:

- Observably show interest in the class activities – whether that is a lecture, class discussions, or activities.

AND

- Contribute a minimum of two comments and/or questions that are relevant to the course topic during a lecture and/or class discussion, and the comments / questions are clearly founded on both the lecture and the reading materials

OR

- Take an active role in leading and/or facilitating discussions / activities during small group discussion s/ activities held during the synchronous class sessions

To earn a *check*, a participant must:

- Observably show interest in the class activities – whether that is a lecture, class discussions, or activities.

AND

- Actively seeks to provide answers to questions being posed to the class, and provides comments relevant to the course topic when elicited.

OR

- Actively participates in discussions / activities during small group discussions / activities held during the synchronous class sessions

Participants will receive a *check-minus* if:

- The participant is visibly disengaged during the synchronous lecture session.

OR

- The participant is visibly disengaged during in-class discussions and activities.

Capstone Exercise Participation:

As the capstone exercise is designed to bring everything that the participants have learned and discussed throughout the course together, all participants are required to attend and participate

throughout the entirety of the capstone exercise, which is scheduled to occur over the last 2 weeks (4 synchronous sessions) of the course. Capstone exercise is a team event, and everyone's learning experience will be enhanced by participants' full participation.

While this is a firm requirement for the participants to successfully complete the course, the instructors and START will work with you on a case-by-case basis to accommodate participants with extenuating circumstances (e.g., unplanned last-minute temporary duty/assignment out of town, or deployment, etc.). Please contact the lead instructor, Dr. Steve Sin (sinss@umd.edu) or training@start.umd.edu if you need assistance in this matter.

If you do not attend and participate throughout the entirety of the Capstone Exercise, and you have not sought out to work with START for extenuating circumstances, you will not be considered to have successfully completed the course, and will not be issued a Certification.
While the participants will not be graded during the capstone exercise in the traditional sense, the instructors will be observing and evaluating each participant based on the following criteria:

- Demonstration of understanding of the course materials (e.g., psychological factors that influence insiders, environmental factors that serves to facilitate insider threat, etc.)
- Demonstrate the ability to critically evaluate a single aspect of the insider threat problem space and present a coherent analysis that contributes to the group completing its tasks
- Demonstrate the ability to examine a complex insider threat questions and identify how they impact and is impacted by organizational, social, economic, legal, and/or ethical dimensions
- Demonstrate the ability to evaluate and recommend for implementation vulnerability reduction measures to achieve the group's goals
- Contribution to any external research needs
- Contribution to completing the group tasks
- Contribution to various aspects of leadership / team membership
- Contribution to resolving conflict within the group

Certification:
A total of 6 Continuing Education Units (CEUs) will be provided to you should you successfully complete the course as outlined above. Certificates will be issued following the completion of the post-test and submission of the final satisfaction survey. Your answers to the satisfaction survey will remain anonymous and not affect your grading. The certificate will be provided to you electronically by the Office of Extended Studies, University of Maryland, College Park.

Course Materials and Navigation:

All materials for this course can be found in the Canvas online course space. You can also access the course by going to Canvas Catalog.

After visiting this site, you will be directed to login. Once you enter your login information, select the appropriate course space, "Novel Approaches to Mixed-Methods P/CVE Research and Practice."

Once you are in the course space, you will have several menu options along the left side of your screen. Below you will find a brief description of the main menu items that you will be using during this course.

- *Home* – The home screen contains a brief introduction to the course.
- *Syllabus* – The most up-to-date syllabus can be found in this section.
- *Announcements* – Any announcements for the course will be posted to this section. Please check regularly.
- *Modules* – The majority of your work will take place in this section. To progress through this course, you must successfully complete each assignment in a module. You will not be able to move on to the next module until you complete all material, successfully participate in the discussion forum, pre and post testing, or the lesson has been opened by the instructor. All assignments and required discussion board posts can also be accessed through this section.
- *Files* – Additional files including readings, as indicated in the lessons, can be found in this section.

Note**:** If this is your first time using Canvas, the E-learning Management System (ELMS) being used for this training, we recommend that you familiarize yourself with this introductory video.

Technical Requirements:

This course is offered through the University of Maryland's online learning platform, Canvas (ELMS). Registration for this course will take place using Canvas Catalog. New Canvas users will create a user account in Catalog during enrollment.

Synchronous Course Platform:

For the synchronous portion, this course will utilize Zoom with live captioning turned on. Zoom link for the synchronous sessions will be provided to the participants in the online course space.

Browsers:

For best performance, Canvas should be used on the current or first previous major release of Chrome, Firefox, Edge, or Safari. Because it's built using web standards, Canvas runs on Windows, Mac, Linux, iOS, Android, or any other device with a modern web browser.
Canvas only requires an operating system that can run the latest compatible web browsers. Your computer operating system should be kept up to date with the latest recommended security updates and upgrades.
Canvas supports the current and first previous major releases of the following browsers:

- **Chrome** 89 and 90
- **Firefox** 87 and 88 (Extended Releases are not supported*)
- **Edge** 89 and 90
- **Respondus Lockdown Browser** (supporting the latest system requirements)
- **Safari** 13 and 14 (Macintosh only)

JavaScript must be enabled to run Canvas.

Browser Security Settings:

Dependent on your browser's security settings, you may be prompted that you are attempting to view insecure content. Known issues that may block mixed content with Canvas can be found on the Canvas support website.

Computer Specifications:

For best performance, you should access Canvas with a computer that supports the most recent browser versions. It is recommended to use a computer five years old or newer with at least 1GB of RAM.

Operating System

Canvas only requires an operating system that can run the latest compatible web browsers. Your computer operating system should be kept up to date with the latest recommended security updates and upgrades.

Internet Speed

Along with compatibility and web standards, Canvas has been carefully crafted to accommodate low bandwidth environments.

It is recommended to have a minimum Internet speed of 512kbps.

Screen Readers

- Macintosh: VoiceOver (latest version for Safari)
- PC: JAWS (latest version for Chrome and Firefox)
- PC: NVDA (latest version for Chrome and Firefox)

Canvas on Mobile Devices:

The Canvas interface was optimized for desktop displays, so using small form factors such as phones may not be a pleasant experience in using Canvas. For the best user experience, please download the Canvas mobile applications. The Canvas mobile applications require Android 6.0 or later and iOS 13.0 or later.

Canvas offers limited support for native mobile browsers on tablet devices. For additional details, please reference the limited-support mobile browser guidelines.

Training Policies:

Copyright – All materials provided in this training course are copyrighted and may not be reproduced for anything other than personal use without written permission from the authors. Please contact us at training@start.umd.edu for more information.

Professional Integrity – All participants are expected to adhere to a level of professional integrity when completing this course. It is expected that the learner will complete all tests and quizzes without assistance.

Accessibility – START strives to provide inclusive programs and encourages participation by individuals with disabilities. To discuss requests for additional accommodations, please contact us at training@start.umd.edu.

A.2: Course Reading List

Course Topic	Reading
Introduction	Proofpoint. (2020). 2020 Cost of Insider Threats: Global Report. Ponemon Institute.
"I" in Insider Threat – The Individual	Dalal, R. S., & Gorab, A. K. (2016). Insider threat in cyber security: What the organizational psychology literature on counterproductive work behavior can and cannot (yet) tell us. In *Psychosocial dynamics of cyber security* (pp. 122-140). Routledge. Greitzer, F. L. (2019, April). Insider Threats: It's the HUMAN, Stupid!. In *Proceedings of the Northwest Cybersecurity Symposium* (pp. 1-8).
"E" in Insider Threat – The Environment	Spector, P.E. (2021, March 23). Don't forget insider threat to cybersecurity. *Paul Spector.* https://paulspector.com/dont-forget-insider-threat-to-cybersecurity/. Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: abundant opportunities for research at the interface. *Journal of business and psychology*, 1-29.
Why are People So Easily Fooled? – Social Engineering	Philipson, J. (2019, July 10). Four reasons why it will be harder to catch the next insider threat. *Homeland Security Today.* https://www.hstoday.us/tag/insider-threats/. Gilovich, T. (1991). Seeing what we want to see: Motivational determinants of belief. *How we know what isn't so: The fallibility of human reason in everyday life*, 75-87. Cialdini, R. B. (2001). The Science of Persuasion. *Scientific American*, *284*(2), 76–81. Sagarin, B. J., & Mitnick, K. D. (2012). The path of least resistance. In D. T. Kenrick, N. J. Goldstein, & S. L. Braver (Eds.), *Six degrees of social influence: Science, application, and the psychology of Robert Cialdini* (pp. 27-38). Oxford University Press.
Identifying and Reporting Threat and Assessing Risk – Better Decision-making	Gilovich, T. (1991). Believing what we are told: The biasing effects of secondhand information. *How we know what isn't so: The fallibility of human reason in everyday life*, 88-111. Philipson, J. (2020, April 22). Improving insider threat detection with evidence-based reporting. *Homeland Security Today.* https://www.hstoday.us/subject-matter-areas/infrastructure-security/improving-insider-threat-detection-with-evidence-based-reporting/. Philipson, J. (2019, November 2). Why 'see something, say something' isn't enough to detect the next insider threat. *Homeland Security Today.* https://www.researchgate.net/publication/337030258_Why_%27See_Something_Say_Something%27_Isn%27t_Enough_for_Next_Insider_Threat.
Risk Management to Address Insider Threat	Bishop, M., Engle, S., Frincke, D. A., Gates, C., Greitzer, F. L., Peisert, S., & Whalen, S. (2010). A risk management approach to the "insider threat". In *Insider threats in cyber security* (pp. 115-137). Springer, Boston, MA.

Course Topic	Reading
	Ivanova, M. G., Probst, C. W., Hansen, R. R., & Kammüller, F. (2013). Externalizing Behaviour for Analysing System Models. *J. Internet Serv. Inf. Secur.*, *3*(3/4), 52-62. Probst, C. W., & Hansen, R. R. (2013). Reachability-based Impact as a Measure for Insiderness. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *4*(4), 38-48. Wang, J., Shan, Z., Gupta, M., & Rao, H. R. (2019). A longitudinal study of unauthorized access attempts on information systems: The role of opportunity contexts. *MIS Quarterly*, *43*(2), 601-622. Shaw, E., & Sellers, L. (2015). Application of the critical-path method to evaluate insider risks. *Studies in Intelligence*, *59*(2), 1-8. ben Othmane, L., Ranchal, R., Fernando, R., Bhargava, B., & Bodden, E. (2015). Incorporating attacker capabilities in risk estimation and mitigation. *Computers & Security*, *51*, 41-61. Zou, B., Yang, M., Guo, J., Wang, J., Benjamin, E. R., Liu, H., & Li, W. (2018). Insider threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation. *Progress in Nuclear Energy*, *104*, 8-15.

A.3: Office of Extended Studies Open Learning Course Application

OFFICE OF EXTENDED STUDIES

Open Learning Non-Credit Course Application

OES-Administration

OES Approval #

Instructions:

- Only one non-credit course per application.
- All fields/questions require a response. If not applicable, please provide an explanation.
- Applications must be submitted at least 30 days prior to the first day of enrollment.
- Commingling between non-credit and credit-bearing courses is not permitted.
- Non-credit courses cannot be offered or advertised until they have been approved.
- Approved applications are valid for one year from enrollment open date (or the approval date for ongoing courses) and may run multiple times within that year if there are no changes. Units must submit a *new Open Learning Non-Credit Course Application* for subsequent offerings at least 30 days prior to expiration.
- Submit the application to oes@umd.edu. After review, the Office of Extended Studies will send your application to the respective dean, chair, and/or division director for signature approval.

Non-Credit Course Information:

Understanding Insider Threat: From Threat to Risk and Trust Course Name	$0 Course Fee
 Previous Approval Number *(If Applicable)*	Steve S. Sin, Judy Philipson, Juliet Aiken Instructor(s) Name
7/26/2021 Course Start Date	9/27/2021 Course End Date
6/6/2021 Enrollment Start Date *(Max Open: 120 Days)*	7/25/2021 Enrollment End Date *(Ref. Appendix A, I.D.b.ii)*
 Primary Contact Name	 Primary Contact Email
 Business Manager Name	 Business Manager Email

KFS# for Revenue Distribution and Billing	Object Code *(Optional)*

Indicate your College/School or Division and your Department/Unit.
Ex: Division: *Academic Affairs*
Unit: *Office of Extended Studies*

Select from list...	
College/School/Division	College/School Dean Name *(Skip for Division)*
Department/Unit:	Division Director or Department Chair Name

OVERVIEW

1. Describe the non-credit offering as it should appear once published. Include all *relevant* details and information. *(Ex: Overview, description, when and where classes meet, instructor name and contact, intended audience, etc.)*

Course Overview:
This course is designed for early career professionals and university students who are interested in the topic of insider threat and how it can be better mitigated.

Course Description:
This course will take the form of a survey course where we will explore past and present trends of insider threat, response and mitigation challenges, and policies, procedures, and practices currently implemented within the U.S. Government to respond to and mitigate threats. The course will also examine individual, organizational, and social stressors that could contribute to insider behaviors and explore the systems approach to countering insider threat. In doing so, the course will expose students to a new paradigm of thinking that shifts the focus from insider threat to insider risk, and from countering insider threat to mitigating insider risk.

Intended Audience:
Early career professionals and university students (undergraduates and graduates) interested in insider threat

Benefit:
The course will increase awareness of the learners about the vast challenges any organization faces in the area of insider threat. The course will provide a foundation from which the learners can develop their own perspectives on insider threat and how best to mitigate it.

Course Delivery Method:
Asynchronous and Synchronous Online Delivery

Instructors:
Dr. Steve S. Sin | sinss@umd.edu | (301) 405-6656
Dr. Judy Philipson | jphilipson@arlis.umd.edu
Dr. Juliet Aiken | jaiken@conducerellc.com

2. Are you working with any external entities to offer the non-credit course?

☐ Yes – Attached a copy of the agreement ☒ No – This course does not involve any external entities

3. Are grants or federal funds being used to cover any costs associated with this course?

☒ Yes – Attached approval from ORA and initial below ☐ No – This course does not utilize any federal funds

___ I confirm that training for any federally funded award is for an award that has gone through the Office of Research Administration (ORA) for approval, and that account set up and training costs associated with this request are an allowable expense for this award.

If applicable, provide additional details regarding the use of any federal funding.

4. The Division of Information Technology (DIT) charges units that use the Open Learning catalog a $10.00 Technology Fee per individual enrolled in a course. If a course is offered free-of-charge to students, faculty, and staff at UMD, units may request a fee-waiver by sending an email to itsupport@umd.edu. Be sure to include: course name and target demographic. *Note: A new waiver approval is required with each application.*

Have you received a fee waiver?

☐ Yes – Attached a copy of the DIT approval ☐ No – This course is not eligible for a waiver

5. Are participants required to pay for the course or is a sponsoring organization paying for all students?

☐ Participants ☐ Sponsor ☒ Payment is not required.

6. If an organization is paying for participants, provide the following:

Org. Name	Address	Contact	Phone	Email

7. Complete the table below for all direct course related expenses. Direct course related expenses include salaries for instructors, graduate assistants, teaching assistants, graders, and guest

speakers who are actively involved in delivering the course. You do not need to include information for indirect course expenses such as salaries for course developers. If the instructor or staff member is not receiving a salary for the course, then an equivalent dollar amount must be determined and provided for the effort put toward this course to ensure state-funded lines are not being used to generate entrepreneurial revenue. *Add additional rows as needed.*

Name	Title	UID	Directory ID	Salary
Dr. Steve S. Sin	Assistant Research Scientist		sinss	
Dr. Judy Philipson	Associate Research Scientist		jphilips	
Dr. Juliet Aiken	Faculty Hourly		jraiken	

8. Would you like OES to contract and pay the instructor and staff?

☐ Yes – OES will process payment ☒ No – My unit will process payment

9. Will this course offer Continuing Education Units (CEUs)?

☒ Yes – Attached the CEU Request Form ☐ No – I will not offer CEUs

ATTESTATIONS

Please initial next to statement indicating that you acknowledge and understand the following:

____ The Office of Extended Studies (OES) provides administrative services for non-credit offerings including program development and delivery, management, student and program services, and financial management. For these services, OES charges the greater of $500 or 10% of gross revenue. I have reviewed and understand the responsibilities of the academic/service unit and those of OES outlined in Appendix A.

____ I understand that the Division of Information Technology (DIT) charges Units that use the Open Learning catalog a $10.00 Technology Fee per individual enrolled in a course. This fee covers contractual and operational costs associated with the learning management system and its integrated learning services/tools. There is an annual cap of $15,000.00 per fiscal year that applies to any academic/administrative unit for which enrollment surpasses 1,500 individuals. Shared and Cross-Listed courses offered by two or more school colleges are not included.

____ I have reviewed the accessibility policies, guidelines, and captioning resources provided in Appendix B. I have used the accessibility checklist to identify any potential accessibility issues and I understand that instructional videos must be captioned for any participant requesting accessibility and disability support. I understand that the academic unit sponsoring the non-credit course is responsible for the cost of any accessibility accommodations.

____ I understand (and will ensure all participants understand) that non-credit courses and Continuing Education Units (CEUs) do not post to the University of Maryland transcript and do not count towards a student's academic record. Neither grade nor credit is earned. Non-credit students do not receive a University ID card nor access to University facilities such as recreation, transportation, and campus events. Non-credit students may access UMD Libraries as Visitors; see https://www.lib.umd.edu/about/visitors.

____ I have read and agree to the terms outlined in the University of Maryland Intellectual Property Policy IV-3.20(A), which delineates ownership and usage rights for materials developed for the non-credit offering.

ATTACHMENT CHECKLIST (if applicable)

☐ Copy of External Entity Agreement

☐ ORA Approval Confirmation

☐ DIT Technology Fee Waiver

☐ CEU Request Form

Appendix A
Overview of Responsibilities
Open Learning Courses Administered by OES

I. OES Administrative Services

A. Program Development and Delivery
   a. Manage the Open Learning catalog processes and procedures.
   b. Assist with completing the mandatory non-credit course application.
   c. Assist with budget development and breakeven projections.
   d. Manage processes for generating, submitting, and administering the External Organization contract as required.
   e. Assist with drafting MOU(s) between UMD and External Organization as needed.
   f. Oversee the approval process and routing for MOUs between UMD and External Organization.

B. Program Management
   a. Provide a point of contact for all administrative services.
   b. Act as a resource for Academic Unit and External Organization on University regulations, policies, and procedures as required.
   c. Oversee Certificate of Completion and awarding of Continuing Education Units as required.

C. Student and Program Services
   a. Scheduling
      i. Enter approved course listing in the Open Learning catalog.
      ii. Assist with campus room reservation as required.
      iii. Manage Open Learning catalog requirements.
   b. Enrollment
      i. Serve as the primary point of contact for student inquires.
      ii. Provide instructions and assistance with Open Learning's online registration system.
      iii. Process all cancellations and withdrawals.
   c. Liaise with Division of IT for troubleshooting student issues.

D. Financial Services
   a. Manage the collection of revenue and net revenue distribution to the program's KFS, with transparent accounting in accordance with the following timeline:

Course Delivery Timespan	Distribution Sent By
September 1 - November 30	March 1
December 1 - February 28	May 1
March 1 - May 31	August 1
June 1 - August 31	November 1

b. Manage all financial transactions including invoicing External Organization or processing student refunds.
    i. OES standard refund policy is a 100% refund until the first day of class access. No refunds are available after the first day of the class access.
    ii. Authorize.net funds are only accessible for 120 days from the participant's enrollment/payment date. Refunds requested after 120 days can take up to 6-8 weeks to process.
c. Coordinate instructor contracting, pay processing, and the reimbursement for instructional support, following University guidelines.
    i. Instructor payment is a one-time payment processed within 30 days of the conclusion of the non-credit course.
    ii. Instructional materials, goods, and/or services (travel, marketing, etc.) are academic unit's responsibility and should be reimbursed via net tuition revenue distribution.

II. Academic/Service Unit Responsibilities

A. Program Development and Delivery
    a. Establish contact with external organizations.
    b. Negotiate content and price for the proposed non-credit offering.
    c. Provide all information in the non-credit course application.
    d. Review and approve proposed non-credit course application budget.

B. Program Management
    a. Liaise with external organizations as required.
    b. Provide information relating to updates/changes to program content and logistics.
    c. Manage curriculum content and instruction including instructor selection.
    d. Provide instructors with requirements for syllabus, textbooks, supplies, class lists, and evaluation of student performance.
    e. Ensure instructors and other staff receive access and training to the Open Learning catalog and ELMS-Canvas. *Resource: UMD Open Learning Administrator Training Course.*
    f. Ensure complete supervision of and arrangements for successful non-credit content delivery including:
        i. Student advising and questions related to the academic aspects of the non-credit offering.
        ii. Reconciling complaints from students dissatisfied with the non-credit offering.
    g. If not offered through the Open Learning catalog, send a finalized class list to OES via email for verification on the first day of class.

C. Financial Management
    a. Provide information required to generate instructor contracts.
    b. Unit is responsible for PHR appointments of all instructors, TA/GAs, hourly employees, and anyone needing ELMS-Canvas access.
        i. For new/initial employees, this includes providing complete information including demographic and education.

ii. For re-employment (following a break in service), update employee information, education, and email.
iii. For those holding a J1 or H1 visa, provide complete employment history, create, and route the visa transaction to PHR.

c. Instructional materials, goods, and/or services costs are the responsibility of the UMD unit. Course supplies will not be reimbursed by OES.
d. Distribution to participating units (if any) is the responsibility of the UMD unit.

Appendix B
Disability and Accessibility Resources

The University of Maryland Web Accessibility Policy sets minimum standards for the accessibility of all university Web-based information used to conduct university business and academic activities to ensure compliance with applicable state and federal regulations. All Web-based information newly adopted or redesigned by any university administrative, academic, or programmatic unit on or after the establishment of this policy must be in compliance with the World Wide Web Consortium's Web Content Accessibility Guidelines (WCAG) Version 2.0 AA conformance level.

Video captioning is mandated primarily for deaf and hard-of-hearing viewers; however, program coordinators and course developers must plan and budget captioning for all prerecorded, live, and audio-described videos.

Resources

(Refer to DIT's Accessibility Services website for the most updated information.)

Policies and Guidelines

- UMD Web Accessibility Policy
- Download Policy Exception Form (PDF)
- UMD IT Accessibility Plan
- Download USM Accessibility Guidelines (PDF)

Video Captioning

- UMD Video Captioning Standard
- How to Caption your Videos
- DIT Captioning Service
- DHHS Captioning Service

UMD Captioning Services

The Division of Information Technology and the Accessibility and Disability Service (ADS) provide services and tools to support the accessibility of UMD courses. Captioning related services include:

- ADS - Deaf and Hard of Hearing Services (contact DHHS for a quote)
- DIT - Panopto Professional Captioning ($1/min for 48h turnaround)

Contact and Support

Contact UMD DIT- IT Accessibility office itaccessibility@umd.edu or 301.405.3364 if you have any questions about these guidelines, how to caption your videos, UMD captioning services, or for a consultation or customized training.

A.4: Office of Extended Studies Open Learning List Details

OFFICE OF EXTENDED STUDIES

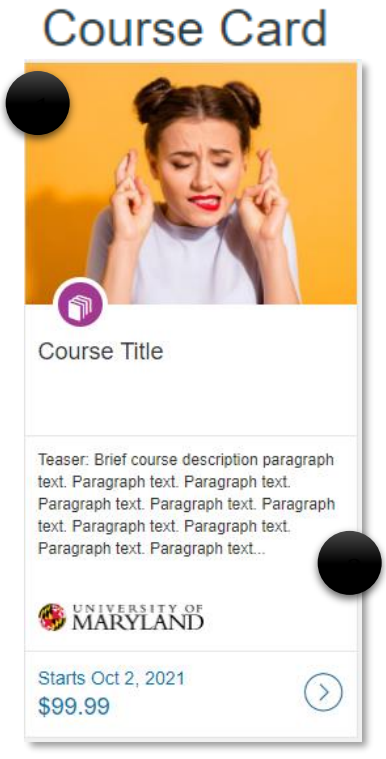
Open Learning Listing Details Information Form

Non-Credit Course Approval Information

Non-Credit Course Application OES Approval #	
Course Name	Understanding Insider Threat: From Threat to Risk and Trust
Course Dates	July 26 – September 27, 2021
Enrollment Dates	June XX – July 25, 2021
College/School/Division	BSOS
Department/Unit	START
Partnership Affiliation Organization	ARLIS, Conducere LLC
Course Enrollment Fee	$0.00
Number of CEUs to be Awarded	6

Storefront Course Card

Reference sample Open Learning non-credit listing Course Card.



1. **Image:** All non-credit offerings in the Open Learning catalog require an image or photo. If you have an image/photo to use, attach it as a separate file when submitting this form along with approval from the owner to use the image for commercial purposes. *For best results, the image should be 768 pixels high and 1,050 pixels wide. Supported Formats: PNG, JPG, GIF, SVG.*

2. **Image Attributes:** Accessibility & Disability alternative (Alt.) text.

Insider Threat

   ☐ No Alt Text (Decorative Image)

3. **Teaser:** A brief paragraph summarizing the non-credit offering. *The teaser text length will appear shortened depending on the size of the screen it is viewed on. Keep the character count brief, with a maximum of 280 characters, including spaces.*

The course examines individual, organizational, and social stressors that contribute to insider behaviors and explore the systems approach to mitigating insider threat. The course will expose students to the paradigm that shifts the focus from insider threat to insider risk

Course Listing Details

Please fill in the fields below with the descriptions as you would like them to appear on the published Open Learning course listing page. ***Leave any fields blank you wish to omit.*

Overview
This course is designed for early career professionals who are interested in the topic of insider threat and how it can be better mitigated.

Course Description
This course will take the form of a survey course where we will explore past and present trends of insider threat, response and mitigation challenges, and policies, procedures, and practices currently implemented within the U.S. Government to respond to and mitigate threats. The course will also examine individual, organizational, and social stressors that could contribute to insider behaviors and explore the systems approach to countering insider threat. In doing so, the course will expose students to a new paradigm of thinking that shifts the focus from insider threat to insider risk, and from countering insider threat to mitigating insider risk.

Benefit
The course will increase awareness of the learners about the vast challenges any organization faces in the area of insider threat. The course will provide a foundation from which the learners can develop their own perspectives on insider threat and how best to mitigate it.

Meet the Instructor		
Name	**Telephone**	**Email**
Dr. Steve S. Sin	**(301) 405-6656**	**sinss@umd.edu**
Instructor Bio		
Dr. Sin is the Director of the Unconventional Weapons and Technology Division (UWT) of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), headquartered at the University of Maryland, where he leads, manages, and develops interdisciplinary research projects spanning across a broad range of national and homeland security challenges. His expertise includes insider threat; adversary behavior modeling; multi-domain operations; emerging technologies and threats; countering weapons of mass destruction; and Northeast Asia regional security. His expertise in Northeast Asia regional security is focused on North Korea, including its nuclear program; cyber capabilities; intelligence apparatus; and regime survival.		

Prior to joining START, Dr. Sin was the Senior Research Associate and Section Chief at the National Center for Security & Preparedness (NCSP) at the State University of New York at Albany, a strategic partner with the New York State Division of Homeland Security & Emergency Services (DHSES). Dr. Sin's extensive experience also includes a career as a U.S. Army Officer.

Meet the Instructor		
Name	**Telephone**	**Email**
Dr. Judy Philipson		**jphilipson@arlis.umd.edu**
Instructor Bio		
Dr. Philipson is an Associate Research Scientist at the Applied Research Laboratory for Intelligence and Security (ARLIS), a University Affiliated Research Center (UARC) at the University of Maryland. She has over 20 years of experience providing behavioral science support to the US Government and private industry clients. Her expertise include: • Risk assessment and insider threat detection • Criminal profiling, counterintelligence assessment, intelligence analysis and information operations • Data-driven tools and strategies to validate sources, methods and data • Qualitative and quantitative research, questionnaire and survey design • Strategic communications, audience analysis and customer segmentation • Customized classes, curricula and tactical training programs		

Meet the Instructor		
Name	**Telephone**	**Email**
Dr. Juliet Aiken		**jaiken@conducerellc.com**
Instructor Bio		
Dr. Aiken is a strategic statistician and organizational change expert who has built and transformed organizations in the academic, private, and public sectors. She created, and served as the founding director of, the Master's in Industrial and Organizational (I/O) Psychology program at the University of Maryland. Dr. Aiken's deepest commitment is to diversifying and improving inclusion in the field of I/O Psychology. Today, as the founder and Chief Consulting Officer of Conducere, LLC, she consults for organizations and build selection systems that improve outcomes for organizations while reducing adverse impact, and drives aligned organizational change around issues related to diversity.		

Time Limit *(Allotted to complete the course.)*	10 Weeks
Length *(Expected time spent.)*	77 Hours
Audience	Young and early professionals

Promotional Discount Codes

Listing Text	*Example: Contact [Name] if you are a member to obtain a $10 discount promotional code.*

Code Details *(Unlimited)*						
	Code *(15 character limit. No spaces. Case insensitive.)*	**Amount**	**Type**	**Usage**	**Start Date**	**End Date**
1			Select...	Select...	Select...	Select...
2			Select...	Select...	Select...	Select...
3			Select...	Select...	Select...	Select...
4			Select...	Select...	Select...	Select...
…			Select...	Select...	Select...	Select...

Other Information to Include *(Indicate if new heading required.)*

Student Cap

25 ☒ Allow Wait List

Canvas Course Access

People to Add *(Add additional rows as needed.)*			
	Name	**Email** *(must have @umd.edu address or *UMD Associate Account)*	**Role**
1	**Steve Sin**	**sinss@umd.edu**	Teacher
2	**Judy Philipson**	**jphilips@umd.edu**	Co-Instructor
3	**Juliet Aiken**	**jraiken@umd.edu**	Co-Instructor
4	**Ron Capps**	**rcapps@umd.edu**	Guest Instructor
5	**Devin Ellis**	**ellisd@umd.edu**	Guest Instructor
6	**Liberty Day**	**lday2@umd.edu**	Course Manager
7	**Kathryn Lindquist**	**klindqui@umd.edu**	Observer

*If anyone outside of UMD needs access, they must first create an associate account. It is key that they 1) Create an associate account, AND 2) Login to Canvas (ELMS) to activate the new account. If they do not login to Canvas first, their account will not be activated and their non-UMD email address will not be recognized. If further "How To" instructions are needed, let us know.

Canvas Resources

Note: The Division of Information Technology (DIT) has a team of designers who are available to collaborate with instructors and academic units to develop an ELMS non-credit course space in Canvas. Fees vary depending upon the offering and the level of support needed. To learn more, email ltdesign@umd.edu or see the DIT Service Catalog.

UMD

- Teaching and Learning Transformation Center (TLTC)
  - TLTC provides faculty, students, and staff with training, resources, professional development activities, and individualized consultation to transform their classrooms and careers. To learn more, email tltc@umd.edu.
- (Re)Design Your ELMS Course--Basics, Open Learning free course
- ELMS-Canvas Faculty Tutorial *(always accessible from within the ELMS course space, as well)*
- Keep Teaching

Canvas / Catalog *(UMD: Open Learning)*

- Canvas Resource Guides

Certificates of Completion

OES only provides Certificates of Completion and CEUs in digital PDF format. If providing a Certificate of Completion or CEUs, complete below:

Choose a design:

☐ Option A: Single Signature

☒ Option B: Double Signature

☒ Print the NAME(s) and TITLE(s) for the signatures as they should appear on the certificate.

1st Signature *(Option A & B)*:

First Name Last Name Title

2nd Signature *(Option B: Double Signature)*:

First Name Last Name Title

Provide jpegs (saved at the highest quality) of the signature(s) and logo(s) as individual attachments. If you select Option B, be sure to provide jpegs for both signatures and both logos. *The recommended image sizes: signature(s) at 300 x 50 pixels; division/college logo(s) at 250 x 50 pixels.*

Checklist:

Individual image attachments included with form submission:

Certificate jpegs		**Course Card**
☐ Signature Image File(s)	☐ Opt. out of Signature Image(s)	☒ Course Image File
☐ Logo Image File(s)	☐ Opt. out of Logo Image(s)	

A.5: Office of Extended Studies Continuing Education Unit Request Form

OFFICE OF EXTENDED STUDIES

Continuing Education Units Request Application

OES Approval #

Instructions:

- Only one non-credit course per CEU request/application.
- All fields/questions/check boxes require a response.
- Applications must be submitted at least 30 days prior to the first day of enrollment.
- Non-credit courses cannot be offered or advertised until they have been approved.
- Approved applications are valid for one year from enrollment open date (or the approval date for ongoing courses) and may run multiple times within that year if there are no changes. Units must submit a new CEU Application for subsequent offerings at least 30 days prior to expiration.
- Submit the application to oes@umd.edu. After review, the Office of Extended Studies will send your application to the respective dean, chair, and/or division director for signature approval.

CEU Course Information

Course Name	Understanding Insider Threat: From Threat to Risk and Trust		
Course Date(s) & Time(s)	July 26 - September 27, 2021		
Location	Online		
Anticipated Enrollment	25		
Total Instructional Hours	60	Total CEUs to be Awarded	6
College/School/Division	BSOS		
Department/Unit	START		
UMD Contact	Should this be Liberty? or Steve?		
Phone		E-mail	
Third Party (if applicable)			
Third Party / Organization Contact			
Phone		E-mail	

Brief Description of Audience	Young and early professionals working in either public or private sectors who are interested in learning more about insider threat and how to better mitigate it.
Program Objectives and Rationale (up to 50 words)	There is an urgent need for us to better understanding of the phenomenon and the ways to mitigate it. This course's aim is to increase learners' understanding of insider threat and ways to mitigate it through the examination of individual, organizational, and social stressors that could contribute to insider behaviors.

Program must meet the following criteria	❑ Learner needs are identified and used as the basis for planned outcomes ❑ Learner outcomes are clear, specific, measurable ❑ Learning outcomes are discussed with students as part of the instructional delivery ❑ Individuals involved in the planning and instructions are competent in the content area and knowledgeable in instructional methods and adult learning processes ❑ Content and instructional methods are appropriate for each learning outcome and accommodate various learning styles ❑ Assessment methods measure achievement of learning outcomes ❑ Learners are provided feedback on their mastery of learning outcomes
Attach a copy of the following: 1. The program agenda showing precise schedule and a sample of the program brochure (if applicable). 2. A clear calculation of qualifying contact hours. Breaks and lunch are not to be included. Refer to the Continuing Education Units (CEU) Guidelines. 3. The program evaluation.	

University of Maryland Unit Approval

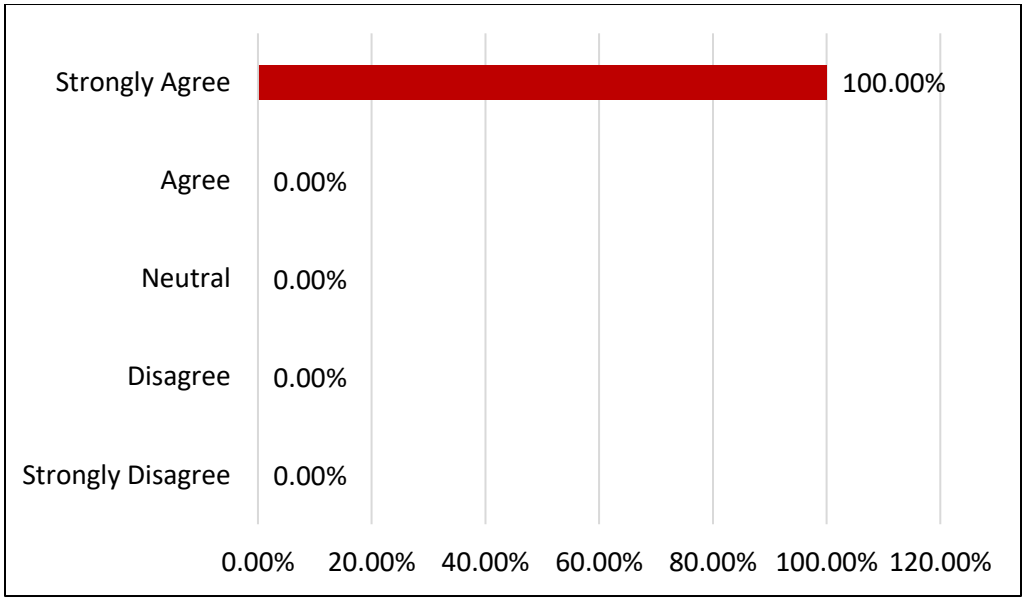
Indicate your College/School or Division and your Department/Unit.
Ex: Division: *Academic Affairs*
Unit: *Office of Extended Studies*

Select from list... College/School/Division	College/School Dean Name *(Skip for Division)*
Department/Unit:	Division Director or Department Chair Name

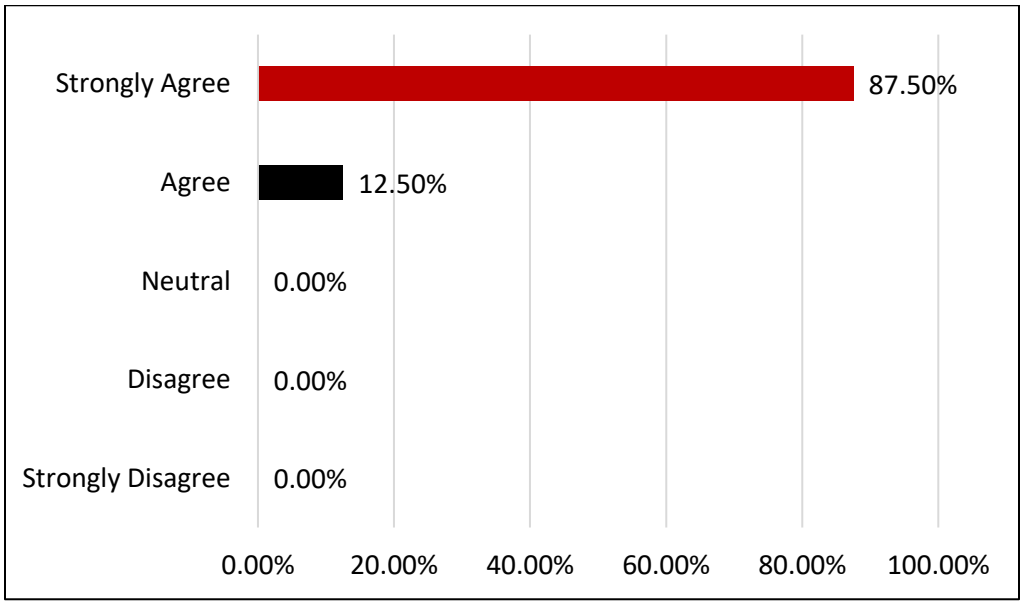
A.6: Post-Course Survey Questions and Results

Closed Ended Questions and Responses

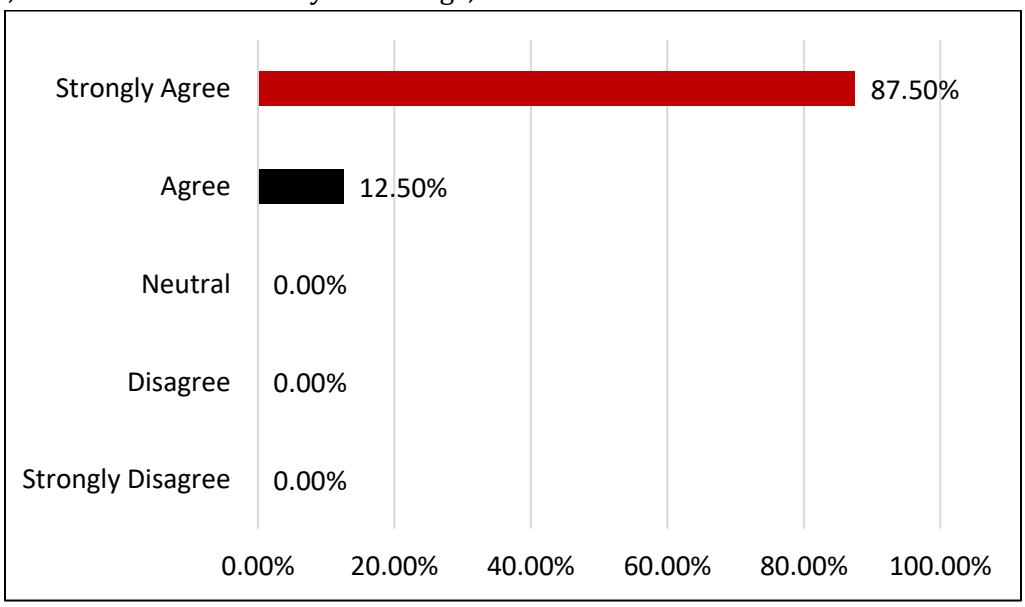
1. I would recommend this course to my peers.



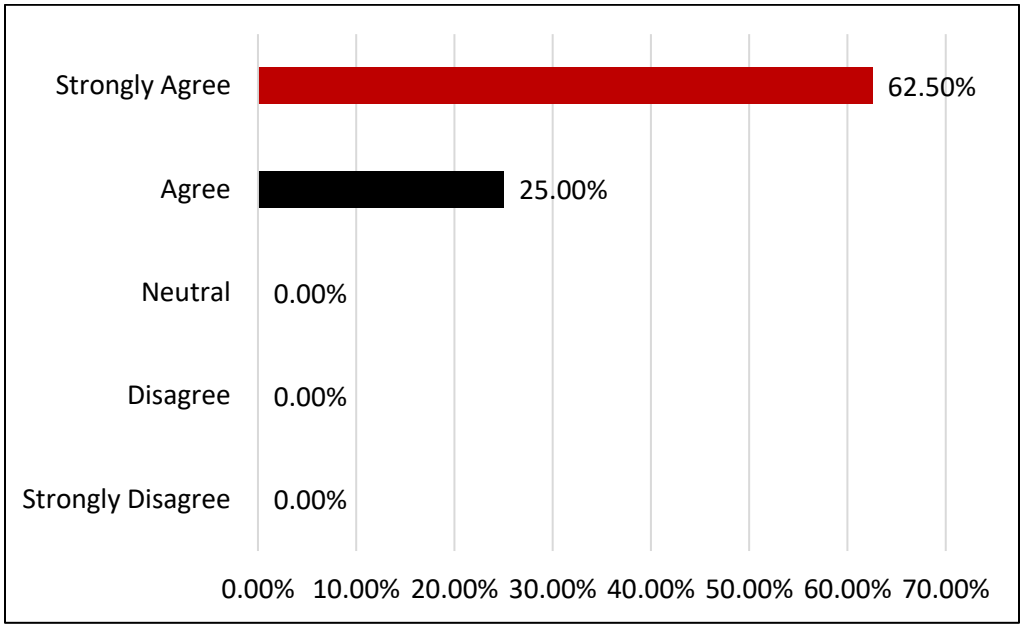
2. Overall, the course met my needs and expectations.



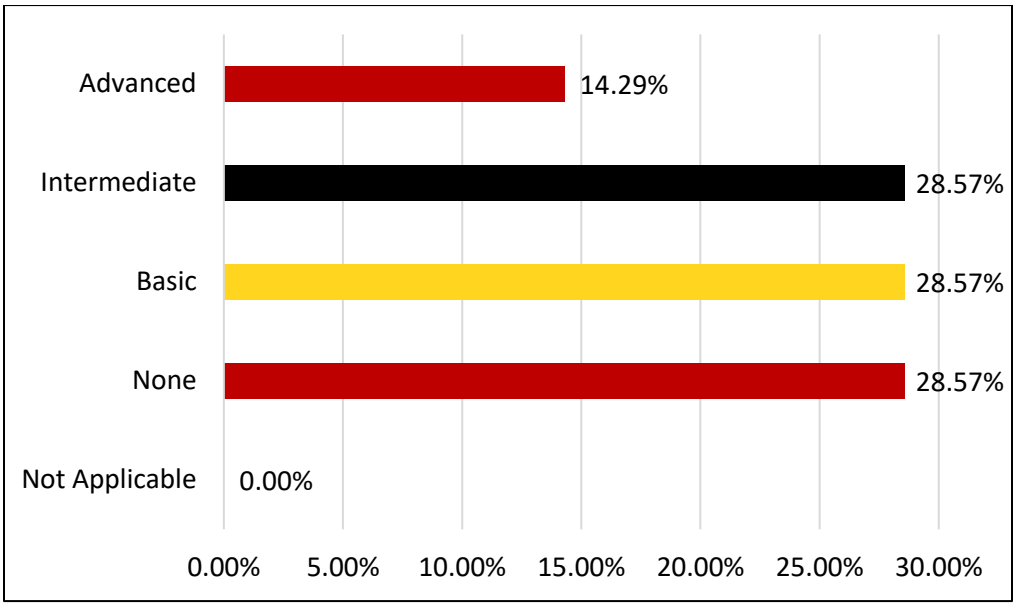
3. Overall, the course increased my knowledge, skills



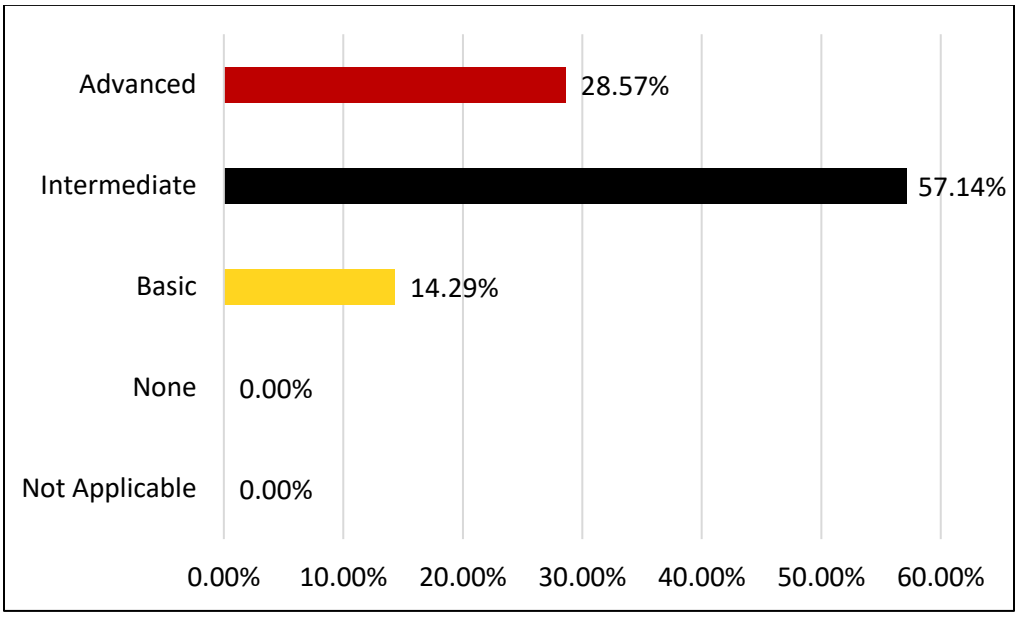
4. The learning activities enhanced learning of course content.



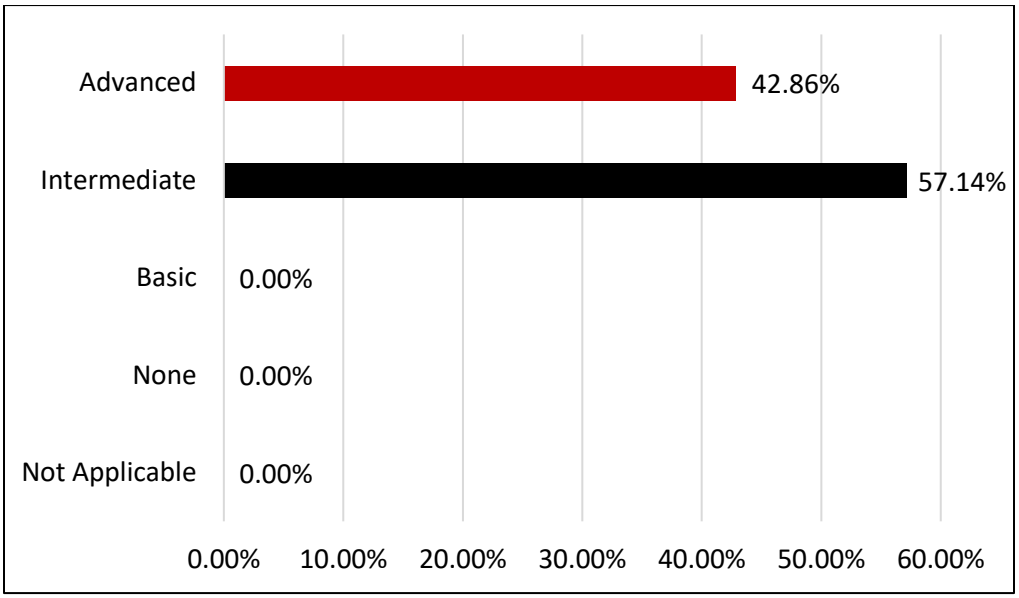
5. PRIOR to completing the training, I would rate my ability to design an insider risk mitigation program as:



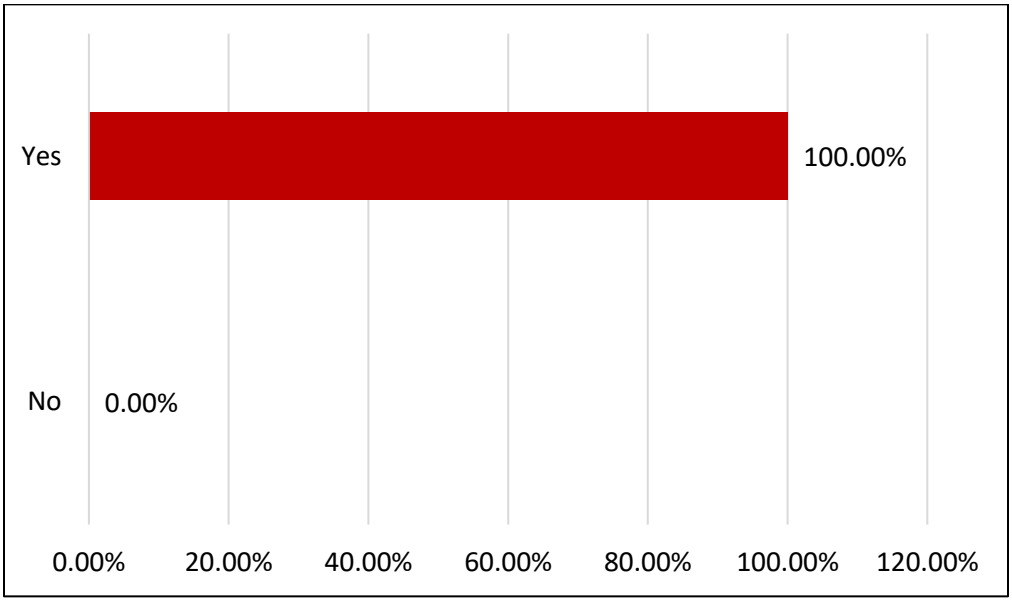
6. AFTER completion of this training, I would rate my ability to design an insider risk mitigation program as:



7. In the FUTURE, as a result of this training, my ability to design a better insider risk mitigation program will be rated as:



8. Do you foresee incorporating what you've learned in this course into your work?



Open Ended Questions and Responses

1. How do you foresee using what you've learned into your work?

- "Understanding the psychology behind insider threat allows me to making the InT program a positive program that can enhance EAP programs while providing organizations better options to mitigate insider threats."
- "I will incorporate professional security measures in my work to guard against insider threats."

- "By consulting risk management approaches/programs with regard to insider threat to our clients on the basis of best practices"
- "General security practices"
- "Theoretically and practically"

2. What are the reasons that you don't foresee incorporating what you've learned into your work?
   - N/A (No response)
3. Which part(s) of the course was/were most valuable to you? Please explain why.
   - "The class discussions, readings, and simulation were most valuable. The class discussions were a great way to see the different perspectives from different professionals. The readings helped to provide the theory behind insider threat concepts. They went into more detail than you'd get with a week-long analyst boot camp type training. I enjoyed the simulation because I like the hands-on approach."
   - "The comments provided by the guest speakers. Their remarks underlined to me why insider threats are of concern across sectors of the economy whether these are in government or private industry."
   - "The psychological and social/behavioral motivators/triggers to become an insider threat-actor"
   - "Theoretical and basic lessons besides capstone exercises"
   - "Listening to different perspectives of insider threat by a diverse group of class participants"
   - "Really enjoyed the class overall"

4. Which part(s) of the course was/were least valuable to you? Please explain why.
   - "Some of the readings that went way into the weeds of formulas and what not were a bit difficult to digest. I think the formulas behind the tools could be their own class."
   - "A very small portion of the readings emphasized the theoretical rather than the practical. Given that the participants were largely professionals some of the assigned readings were less useful for these individuals."
   - "The math equation/formula to determine the likeliness of insider threat"
   - "ICONS platform navigability"
   - "None"
   - "I have no complaints"

5. General comments: Please provide any other comments or suggestions below.
   - "Overall, I liked how the class was run. I took DIA's week-long analyst course, and I think this class could be a follow up course to that. The DIA analyst course made you familiar with identifying certain elements to look for and how to respond appropriately. This course got into the why behind what motivates people and what affects our biases as analyst."
   - "I thoroughly enjoyed this class. The diversity of course instructors was a strong point. By far and away the most advantageous aspect was the range of students in the course."

- “Good comprehensive course, with much interaction between participants, extensive readings about subjects and enthusiastic teaching mode.”
- “More teachers can be involved from the real life as doing this insider threat issue.”
- “In general I thought it was a good class, as a 'beta' class there are always areas needing tightening up; for a class as this one was that was composed of professionals in the field or closely related field the less demanding constraints place on having to get the pre- post survey tests completed, or discussion posts completed by a specific time was good. Also, as a former adjunct I would like to say that I felt that there was a higher-than-normal drop-out rate, BUT, hey, those who just faded away missed out on an enjoyable class.”