National Model Curriculum for Programs in Intelligence and Cybersecurity

Bachelor of Science in Information Systems Technology (Cybersecurity, Intelligence Option)
Master of Science, National Cyber Security Studies

Summary

This model curriculum serves as a contribution to the current on-going effort of preparing Intel/Cybersecurity professionals with the dual competencies needed in the two areas in order to protect our nation from the 21st century cyber challenges we face. We provide templates for two programs: Bachelor of Science in Information Systems Technology (Cybersecurity, Intelligence Option) and the Master of Science in National Cyber Security Studies. Whereas we draw from two existing programs, we have tried to make this contribution as generic as possible. The templates include: (1) analysis and integration of the Office of the Director of National Intelligence's (ODNI) Intelligence Community Directive (203) (ICD 2003, January 2015) competencies to the NICE Cybersecurity Workforce Framework (November 2016) competences (2) framework for model course generation using ODNI ICD 203 and NICE KSATs, (3) alignment of Institutional Learning Outcomes/Program Learning Outcomes/Student Learning Outcomes for the BSc Cyber Intelligence program (4) alignment of Institutional Learning Outcomes/Program Learning Outcomes/Student Learning Outcomes for the MSc Cyber Intelligence program. (5) additional Insights on Lessons Learnt from adopting the model curriculum.

To graduate with the BSc degree, undergraduate students must compete 180 units as follows: General Education (88 Units); Lower Division Requirements (36 Units); Upper Division (28 units) and Intelligence Option (28 Units). To graduate with the MSc degree, students must complete 56 to 58 units to graduate (not including the 12 Units pre-requisite courses): Core Courses (20 Units); Cybersecurity Courses (24 Units); Elective Courses (12 Units) and Culminating Experience Course (0 – 2 Units). Two departments share the primary responsibility for the degree program: Political Science Department (National Security Studies) in the College of Social and Behavioral Sciences, and Information and Decision Science Department (Cybersecurity) in the College of Business and Public Administration.

Program Rationale

Both degree programs prepare students for career paths in Cybersecurity Intelligence. The goal is to address the "shortage of professionals within the IC that have cybersecurity technical knowledge." A graduate from the BS or MS program could work as: All-Source Analyst, Warning Analyst, Mission Assessment Specialist, Target Developer, Target Network Analyst, Cyber Defense Analyst, Vulnerability Assessment Analyst, Multi-Disciplined Language Analyst, All-Source Requirements and Collection Manager, Cyber Intel Planner, Cyber Ops Planner, Partner Integration Planner, Cyber Operator, Cyber Crime Investigator, Forensic Analyst, and Cyber Defense Forensic Analyst. Career paths for the MS degree graduates may lead to strategic positions such as Chief Information Officer, Chief Information Security Officer, Chief Compliance Officer, Chief Data officer, or Chief Cybersecurity Architect. Once they are hired, additional training may be required to get graduates acquainted with specific tools and work processes as needed.

The undergraduate program is open to all qualified students majoring or minoring in political science, public administration, cybersecurity, information systems technology, computer science, or a related field. Qualified transfer students from community colleges or other accredited university programs also qualify. Students applying for the master's program must have a baccalaureate degree from an accredited college or university; demonstrate preparation to succeed in graduate study, submit GRE scores, complete a graduate entrance

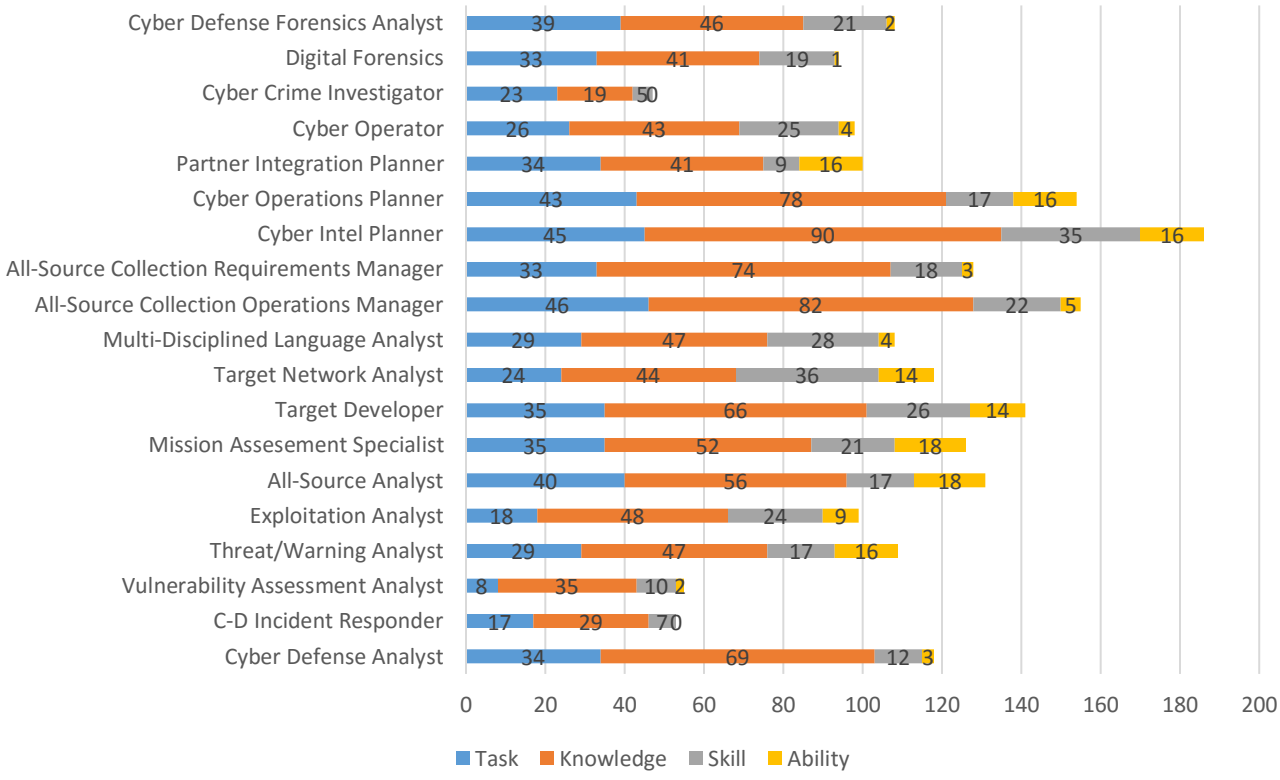
writing requirements and must have a 2.5 overall undergraduate GPA and at least 3.0 GPA in the undergraduate major.

Graduating BSc or MSc students must demonstrate ability to think critically within the intelligence life cycle, fuse intelligence and cybersecurity operations, use analytic tradecraft standards to analyze intelligence and cybersecurity issues, and show a keen desire to protect our nation against cybersecurity threats and attacks.

1. Analysis and integration of NICE- CWF and ODNI IDC 203 Competencies

As should be expected, the traditional competencies required for cybersecurity professionals and those required for IC professionals come from different domains. The NICE Cybersecurity Workforce Framework (November 2016) from the National Institute of Science and Technology (NIST) mainly provides the source for competencies [Knowledge, Skills, Abilities and Tasks(KSATs)] required for cybersecurity professionals whereas competencies required for intelligence professionals are spelled out in the Office of the Director of National Intelligence's (ODNI) Intelligence Community Directive (203) (ICD 2003, January 2015). A quick analysis the KSAs in two (2) categories in the NICE Cybersecurity Workforce Framework[1] (AN-Analyze[2]; and CO-Collect and Operate[3]) whose work roles seem to overlap with intelligence analysis show a low relationship to intelligence analysis: Knowledge (K) has only 2.8% clearly related; Skills (S) has about 15% clearly related; and Abilities (A) has about 26% clearly related to intelligence analysis.

Table 1: Frequency of NICE KSATs Cybersecurity Intelligence Work Roles



However, an analysis of the combination of the competencies required for a Cybersecurity Intelligence professional presents different picture because it involves the blending of the two domains.

---

[1] See Appendix 1 for a detailed analysis of ODNI ICD 203 Intelligence Analysis Competency Requirements.

[2] **Analyze (AN)**—Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

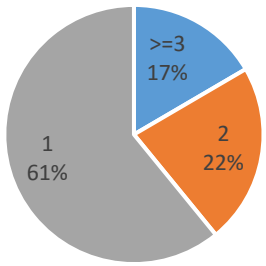
[3] **Collect and Operate (CO)**—Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

1.1. Analysis of NICE-CWF Competencies

Table 1 shows the frequency count of KSATs in the NICE –CWF Cybersecurity Intelligence Work Roles. In addition to work roles from the Analyze (AN) and Collect and Operate (CO) categories, we have included KSATs from the Protect and Defend (PR) and Investigate (IN) categories that also overlap cybersecurity intelligence activities.

The total composition of NICE KSAT items in the AN, CO, PR & IN Cybersecurity Intelligence categories is as follows: Knowledge (47%), Skill (17%), Ability (8%), and Tasks (28%). An analysis of this spread (Shown in Figure 1) indicates that whereas 61% of the KSATs are specialized and specifically assigned to one (1) work role only i.e., they appear only once; 22% are assigned to two (2) work roles, and 17% are assigned to three (3) or more work roles. Which means, 39% of the KSATs in the Cyber Intel categories are cross-listed in at least two work roles. Items with the highest cross-listed frequency are in Knowledge (five items found in each work role), followed by Ability (with two items included in ten (10) work roles, then Skill (with one item include in eight (8) work roles, and last, Task (with two items listed in five (5) work roles).

Figure 1: Overall Frequency NICE Items for Cyber/Intel Work Roles



Figures 2 through 5 show that sixty four percent 64%) of the NICE Ability items are cross-listed in 2 or more work roles, followed by fifty five percent (55%) for Knowledge items, 35% for Skill items, and 18% for Task items. The implication is that cyber intelligence programs should consider creating core-requisite courses based on high cross-listed KSATs. Highly cross-listed KSATs indicate potential areas for core-requisite threshold concepts in curriculum development. Similarly, items listed only once are candidate items for specialization courses. The high percentage of Ability and Knowledge cross-listed KSATs suggests that development of Abilities and inculcation of Knowledge are key to Skill growth and Task performance.

Figure 2: Frequency of Ability NICE Items for Cyber/Intel Work Roles

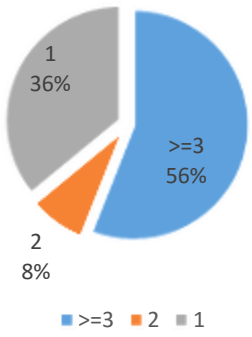


Figure 3: Frequency of Knowledge NICE Items for Cyber/Intel Work Roles

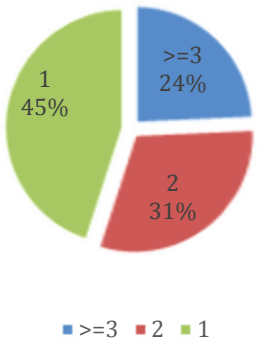


Figure 4: Frequency of Skills NICE Items for Cyber/Intel Work Roles

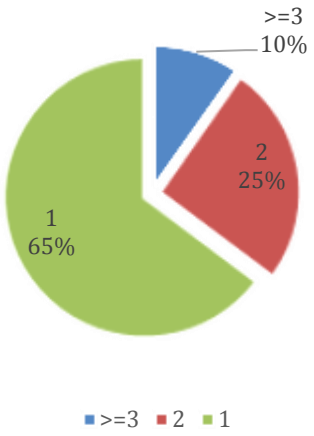
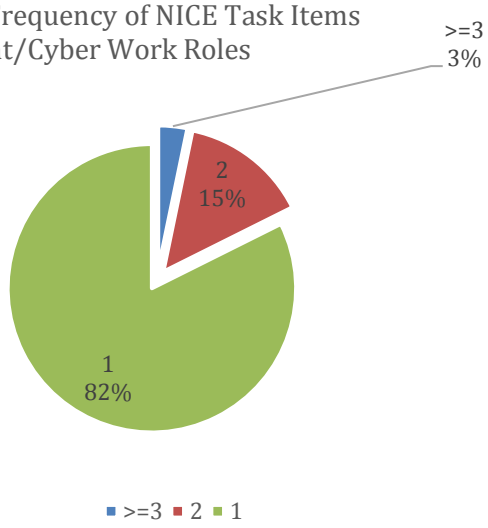


Figure 5: Frequency of NICE Task Items Int/Cyber Work Roles



1.2 Analysis of ODNI IDC 203 Competencies

As described in Appendix 1, the source for the IC workforce competencies are provided in the Office of the Director of National Intelligence's (ODNI) Intelligence Community Directive (ICD) 203. According to ICD 203, the IC workforce must exemplify the following five Analytic Standards: (1) Objectivity, (2) non-partisan, (3) timely, (4) use all available sources of intelligence, and (5), exhibit the following nine (9) specific Analytic Tradecraft Standards:

1) Describes quality and credibility of underlying sources, data, and methodologies
2) Expresses and explains uncertainties associated with analytic judgments
3) Distinguishes between underlying intelligence information and analysts' assumptions and judgments
4) Incorporates analysis of alternatives
5) Demonstrates customer relevance and addresses implications
6) Uses clear and logical argumentation
7) Explains change to or consistency of analytic judgments
8) Makes accurate judgments and assessments
9) Incorporates effective visual information where appropriate

Since the Analytic standards are not required for entry level intelligence analysts yet, and they do not indicate how to prepare students for intelligence careers, the National Center for Security Studies conducted a study in November 2016 to assess the general/common skills required for entry-level positions across a number of intelligence agencies.

Table 2: Frequency of General/Common Skills Required by Various Intel Entry-Level Jobs

Code	General/Common Skills	% Agencies requiring
CW	Clear Writing	100%
OC	Clear oral communication	95%
AD	Analyze data/information	95%
AE	Analyze alternative explanations	80%
IG	Identify information gaps	40%
TW	Team work/collaboration	30%
RG	Regional/Geographic knowledge	30%
LG	Language skills (preferred, not required)	30%

1.3 integration of NICE- CWF and ODNI IDC 203 Competencies

A noun/verb analysis of the General/Common skills provided by ODNI- ICD 203 competencies yielded 78 KSATs: Ability (22 items), Knowledge (2 items), Skills (12 items), Tasks (42 items). A text analysis of the KSAT items provided the following frequencies: Team/Collaborate/Collaboration (22 times), write/writing (8), analyze/analysis (27), disseminate/present/oral communication (9), Gaps (7), intelligence (15). This means that the blending of the NICE-CWF KSATs and the ODNI-IDC competencies provide us the opportunity to prepare Intel/Cybersecurity professionals with the dual competencies needed in the two areas in order to protect our nation for the 21st century cyber challenges we face.

2. A Framework for Model Course Generation using ODNI-ICD 203 and NICE-CWF KSATs

The NICE –CWF and the ODNI-ICD 203 guidelines provide a starting point for developing courses that will offer our students the various career pathways to eventually serve in the work roles they yearn for. Nevertheless, no academic program can cover all the KSATs. Which means each academic program must prioritize and select KSATs based on their CAE designation, institutional support and resources, accreditation requirements, and the skills and experience of their faculty. One way to do this is to use the standard 'MoSCoW' technique used in new program/product development and Use Case Requirements Modeling:

Must Have: those are work roles and KSATs that must be pursued in the current program
Should Have: those are work roles and KSATs that are important but not necessary for the time being. They could be added to the program in due course
Could Have: those are work roles and KSATs that are desirable but will not be part of the program
Won't Have: those are work roles and KSATs that are not appropriate for our program for the time being

We have included Cyber Intel Generic Course Generation Template "Cyber-Intel Generic Course Generation MoSCoW Template fin.xlsx" you can use to guide your course development. This activity should be done by a team of Subject Matter Experts preferably composed of instructional designers and the instructors who will be responsible for teaching the course. The Excel Cyber Intel Generic Course Generation Template provides options to use the NICE-CWF KSATs to develop five courses in the following Intel Competency Areas:

- Communication & Communication Tools—this acknowledges that human to human communication should be supported by IT tools:-- human to computer communication, computer to computer, and computer to human
- Analyze – Analysis of data/information and alternative explanations
- Team Work/Collaboration – understanding of group dynamics, team creative problem solving, individual creative problem solving styles, fostering behavioral excellence in group dynamics
- Research – gap analysis, targets, questions, design, collection, organization, analysis, conclusions, presentation
- ICD-203 – specialized privileged courses offered for specific purposes

3. Alignment of Institutional Learning Outcomes/Program Learning Outcomes/Student Learning Outcomes for the BSc Cyber Intelligence program

Below we have provided a Template that can be repurposed and used for preparing a BSc Cyber Intelligence degree program. This generic template shows how the ILO/PLO/SLO could be developed and operationalized as a basis for assessing student learning. A completed proposal ready for submission will depend on your institution requirements. We have also provided an excel file: "Final Syllabus Analysis Template-3.xlsx" that shows some of the courses we referenced in this generic template. This will help in understanding how we put the alignment template together.

Table 1: Alignment of Institutional Learning Outcomes and Program Learning Outcomes—BSc IST Cyber Intelligence

Institutional Learning Outcomes	Program Learning Outcomes
ILO1. Breadth of Knowledge: Students identify, explain, and apply multiple approaches to problem solving and knowledge production within disciplines, across disciplines and fields to intellectual, ethical, social, and practical issues.	PLO1. Specific Knowledge and Skills: Each student will obtain specialized knowledge and skills on how to apply analytic tradecraft standards and cybersecurity tools to identify, collect, organize and analyze well-sourced data to provide accurate judgements and assessments to target customers and policy makers. PLO 2. Communication: Each student will employ specific Analytic Tradecraft Standards and available information systems technology to communicate clearly and objectively (oral or written) with organizational stakeholders on cybersecurity and intelligence issues to ensure attainment of specified local, state, national, and international strategic objectives
ILO2. Depth of Knowledge: Students demonstrate a depth of knowledge in a specific discipline or field and apply the values and ways of knowing and doing specific to that discipline or field to intellectual, ethical, social, and practical issues.	
ILO3. Critical Literacies. Students analyze the ways artistic, oral, quantitative, technological and written expression and information both shape and are shaped by underlying values, assumptions and contexts, so that they can critically contribute to local and global communities.	
ILO4. Ways of reasoning and inquiry. Students engage in diverse methods of reasoning and inquiry to define problems, identify and evaluate potential solutions, and determine a course of action.	PLO 3. Problem solving with Information Systems Technology: Each student will apply IST knowledge and structured intelligence analysis techniques to assess unforeseen events and unfamiliar circumstances and devise innovative solutions to solve problems at the local, state, national and international levels including: cyber defense/offence, vulnerability assessment, exploitation analysis, all-source analysis, mission assessment, target analysis, database security, and cybercrime investigation and litigation.
ILO5. Creativity and Innovation. Students develop and use new approaches to think, solve problems, and express themselves.	
ILO6. Integrative Learning. Students connect disciplines and learning experiences to frame and solve unscripted problems using lenses from multiple fields, contexts, cultures and identities.	
ILO7. Engagement in the Campus, Local and Global Communities. Students develop dispositions and apply intellect and behaviors to respect and promote social justice and equity on campus and across local and global communities.	PLO 4. Ethical Reasoning in a Global Context: Each student will identify, evaluate and discuss ethical and regulatory cybersecurity issues at an individual, professional, organizational, local, state, national and global context.
ILO8. Diversity and Inclusion. Students understand how dynamics within global communities influence the ways in which people see the world. They develop dispositions to respectfully interact and collaborate with diverse individuals and groups and acknowledge their own perspectives and biases.	

Table 2: Alignment of Program Learning Outcomes, Student Learning Outcomes, Where Taught and Where the SLO is Assessed			
Program Learning Outcomes	**Student Learning Outcomes**	**Where Taught**	**Where the SLO is Assessed**
PLO1. Specific Knowledge and Skills: Each student will obtain specialized knowledge and skills on how to apply analytic tradecraft standards and cybersecurity tools to identify, collect, organize and analyze well-sourced data to provide accurate judgements and assessments to target customers and policy makers.	SLO1. The student shall integrate knowledge obtained in the program by using structured analytic techniques and cybersecurity tools to undertake a comprehensive class project that addresses a real, substantive cybersecurity/intelligence related problem.	All Program courses	IST 490: Information Systems Planning and Policy
	SLO2. The student shall integrate the knowledge of the area (Cybersecurity, National Security Policy, American Foreign Policy, International Relations Theories), to show critical and independent thinking, and demonstrate mastery of the subject matter.	PSCI 325: American Foreign Policy PSCI 204: International Relations Theories PSCI 484: National Security Policy PSCI 590: Techniques of Intelligence Analysis	PSCI 590
PLO 2. Communication: Each student will employ specific techniques of intelligence analysis and available information systems technology to communicate clearly and objectively (oral or written) with organizational stakeholders on cybersecurity and intelligence issues to ensure attainment of specified local, state, national, and international strategic objectives	SLO1. The student shall integrate knowledge obtained in the program by using structured analytic techniques and cybersecurity tools to undertake a comprehensive class project that addresses a real, substantive cybersecurity/intelligence related problem.	All Program courses	PSCI 590 or IST 490
PLO 3. Problem solving with Information Systems Technology: Each student will apply IST knowledge in new and unfamiliar circumstances and devise innovative solutions to solve business problems and cope with unforeseen events including analyzing IST organizational needs, designing and implementing secure IST applications, cyber defense/offence, risk management, securing networks, and cybercrime investigation and litigation.	SLO3. The student shall understand and apply appropriate cybersecurity tools and intelligence techniques to identify, collect, analyze, and transform data into accurate information for presentation to target stakeholders.	IST 525: Computer Forensics IST 415: Security Systems Management IST 511: Cyber Defense IST 215: Cyber Security IST 275: Information Networking & Security	PSCI 590 or IST 490
	SLO4. The student shall understand, select, and apply appropriate technologies, policies, and procedures (including forensic tools) needed to assure the confidentiality, integrity, and availability of information systems.	IST 525: Computer Forensics IST 415: Security Systems Management IST 309: Advanced Information Networking and Security IST 511: Cyber Defense	
	SLO5. The student shall understand business models and identify a business (IST) problem, analyze (IST requirements, and apply secure design principles used in information systems development and implementation projects.	IST 309: Information Systems and Technology Management IST 474: Advanced Database Management & Policy IST 515/SCM 515: Project Management	
	SLO6. The student shall understand enterprise information systems, technology architectures, and the IST governance processes.	IST 490: Information Systems Planning and Policy	
PLO 4. Ethical Reasoning in a Global Context: Each student will identify, evaluate and discuss ethical and regulatory cybersecurity issues at an individual, professional, organizational, local, state, national and global context.	SLO7. The student shall understand and integrate the legal, ethical, and global implications of IST as it relates to Cybersecurity at an individual, professional, organizational, local, state, national and international context	PSCI 204: International Relations Theories MGMT 302: Management and Organizational Behavior MGMT 230: Business Law PSCI 484: National Security Policy	PSCI 590 or IST 490

Table 3a:
Summary Matrix showing where student learning outcomes are introduced (I), developed (D) and mastered (M)

	PSCI 204	PSCI 325	PSCI 484	ADMIN 210	IST 101	IST 215	IST 274	IST 275	IST 276	IST 282	MGMT 230	IST 309	IST 372
SLO1.	**I/D**	**D**	**D**	**I/D**	**D**	**I/D**	**I/D**	**I/D**	**I/D**	**I/D**	**I/D**	**D**	**D**
SLO2	**I/D**	**D**	**I/D**	**I/D**	**D**	**D**	**D**	**I/D**	**I/D**	**I/D**	**I/D**	**D**	**I/D**
SLO3						**I/D**		**I/D**					
SLO4						**I/D**		**I/D**				**D**	
SLO5							**I/D**		**D**			**D**	
SLO6					**D**							**D**	
SLO7	**I/D**		**I/D**								**I/D**		

Table 3b:
Summary Matrix showing where student learning outcomes are introduced (I), developed (D) and mastered (M)

	MGMT 302	IST 474	IST 415	IST 511	IST 515	IST 525	IST 490	IST 590
SLO1.		**D**	**D**	**D**		**D**	**M**	
SLO2								**M**
SLO3			**D**	**D**		**I/D**	**M**	**M**
SLO4			**D**	**D**		**I/D**	**M**	**M**
SLO5		**D**			**I/D**		**M**	**M**
SLO6							**D/M**	**M**
SLO7	**I/D**						**M**	**M**

Summary of Direct Assessment Measures:

Outcomes	**Class**	**Method**
Specific Knowledge and Skills	PSCI 590 IST 490	Applied Project Final Exam
Communication	PSCI 590 IST 490	Applied Project Final Exam
Problem Solving with Information Technology	PSCI 590 IST 490	Applied Project Final Exam
Ethical Reasoning in a Global Context	PSCI 590 IST 490	Applied Project Final Exam

Summary of Indirect assessment measures:

- Bi-annual Assurance of Learning Reports and Faculty Forums
- Bi-annual CIR Reports
- Syllabus Analysis
- Internship Survey
- Employer Survey
- Student Survey
- Assessment Center

EXHIBIT ##: (B.S.) INFORMATION SYSTEMS AND TECHNOLOGY INTELLIGENCE OPTION ROADMAP

YEAR 1 (<45 units)

Quarter 1	Quarter 2	Quarter 3
☐ IST 101	☐ IST 215	☐ IST 274
☐ GE A-1 (English)	☐ GE A-2 (COMM 120)	☐ GE A-3 (Critical Thinking)
☐ GE B-1 (Math110)	☐ GE B-2 (Life Science)	☐ GE C-2 (Literature)
☐ GE E-2 (FIN 101)	☐ GE- E1 (KINE 205)	☐ GE D-3 (World Cultures)

YEAR 2 (45-90 units)

Quarter 1	Quarter 2	Quarter 3
☐ IST 275	☐ IST 276	☐ IST 282
☐ GE C-1 (Arts)	☐ MGMT 230	☐ GE B-3 (Physical Science)
☐ GE D-1 (American History)	☐ GE D-2 (PSCI 203)	☐ GE C-4 (Philosophy)
☐ GE B-4 (Special Topics) ☐ GE E-3 (Physical Education)	☐ GE C-3 (Foreign Language)	☐ GE D-4 (Discipline Perspective)

YEAR 3 (90-135 units)

Quarter 1	Quarter 2	Quarter 3
☐ IST 309	☐ IST 372	☐ IST 415
☐ ADMN 210	☐ IST 475	☐ PSCI 484
☐ MGMT 306	☐ PSCI 204	☐ IST 474
☐ MGMT 302	☐ UD GE Capstone	☐ UD GE Capstone

YEAR 4 (>135 units)

Quarter 1	Quarter 2	Quarter 3
☐ SCM 515	☐ IST 525	☐ IST 490
☐ IST 511	☐ PSCI 325	☐ PSCI 590
☐ UD GE Capstone	☐ Free Elective (if needed)	☐ Free Elective (if needed)
☐ Free Elective (if needed)		

4. Alignment of Institutional Learning Outcomes/Program Learning Outcomes/Student Learning Outcomes for the MSc Cyber Intelligence program.

Again, below we have provided a Template that can be repurposed and used for preparing a MSc Cyber Intelligence degree program. This generic template shows how the ILO/PLO/SLO could be developed and operationalized as a basis for assessing student learning. Obviously, more will need to be done to have a complete proposal ready for submission based on your institution requirements.

Table 1: Alignment of Institutional Learning Outcomes and Program Learning Outcomes—MSc Cyber Intelligence	
Institutional Learning Outcomes	Program Learning Outcomes
ILO1. Breadth of Knowledge: Students identify, explain, and apply multiple approaches to problem solving and knowledge production within disciplines, across disciplines and fields to intellectual, ethical, social, and practical issues.	PLO1. Specific Knowledge and Skills: Each student will obtain specialized knowledge and skills on how to apply analytic tradecraft standards and cybersecurity tools to identify, collect, organize and analyze well sourced data to provide accurate judgements and assessments to target customers and policy makers. PLO 2. Communication: Each student will employ specific Analytic Tradecraft Standards and available information systems technology to communicate clearly and objectively (oral or written) with organizational stakeholders on cybersecurity and intelligence issues to ensure attainment of specified local, state, national, and international strategic objectives
ILO2. Depth of Knowledge: Students demonstrate a depth of knowledge in a specific discipline or field and apply the values and ways of knowing and doing specific to that discipline or field to intellectual, ethical, social, and practical issues.	
ILO3. Critical Literacies. Students analyze the ways artistic, oral, quantitative, technological and written expression and information both shape and are shaped by underlying values, assumptions and contexts, so that they can critically contribute to local and global communities.	
ILO4. Ways of reasoning and inquiry. Students engage in diverse methods of reasoning and inquiry to define problems, identify and evaluate potential solutions, and determine a course of action.	PLO 3. Problem solving with Information Systems Technology: Each student will apply IST knowledge and structured intelligence analysis techniques to assess unforeseen events and unfamiliar circumstances and devise innovative solutions to solve problems at the local, state, national and international levels including: cyber defense/offence, vulnerability assessment, exploitation analysis, all-source analysis, mission assessment, target analysis, database security, and cybercrime investigation and litigation.
ILO5. Creativity and Innovation. Students develop and use new approaches to think, solve problems, and express themselves.	
ILO6. Integrative Learning. Students connect disciplines and learning experiences to frame and solve unscripted problems using lenses from multiple fields, contexts, cultures and identities.	
ILO7. Engagement in the Campus, Local and Global Communities. Students develop dispositions and apply intellect and behaviors to respect and promote social justice and equity on campus and across local and global communities.	PLO 4. Ethical Reasoning in a Global Context: Each student will identify, evaluate and discuss ethical and regulatory cybersecurity issues at an individual, professional, organizational, local, state, national and global context.
ILO8. Diversity and Inclusion. Students understand how dynamics within global communities influence the ways in which people see the world. They develop dispositions to respectfully interact and collaborate with diverse individuals and groups and acknowledge their own perspectives and biases.	

Table 2: Alignment of Program Learning Outcomes, Student Learning Outcomes, Where Taught and Where the SLO is Assessed			
Program Learning Outcomes	**Student Learning Outcomes**	**Where Taught**	**Where the SLO is Assessed**
PLO1. Specific Knowledge and Skills: Each student will obtain specialized knowledge and skills on how to apply analytic tradecraft standards and cybersecurity tools to identify, collect, organize and analyze well sourced data to provide accurate judgements and assessments to target customers and policy makers.	SLO1. The graduate student shall integrate knowledge obtained in the program by using analytic tradecraft standards and cybersecurity tools to undertake a comprehensive research project that addresses a real, substantive cybersecurity/intelligence related problem.	All Program courses	PSCI 699: MS Culminating Project
	SLO2. The graduate student shall integrate the knowledge of the area (Cybersecurity, Strategic Intelligence, National and International Security, Analytic Tradecraft etc.), show critical and independent thinking, and demonstrate mastery of the subject matter.	All Program Courses	PSCI 999: MS Culminating Comprehensive Exam
PLO 2. Communication: Each student will employ specific Analytic Tradecraft Standards and available information systems technology to communicate clearly and objectively (oral or written) with organizational stakeholders on cybersecurity and intelligence issues to ensure attainment of specified local, state, national, and international strategic objectives	SLO1. The graduate student shall integrate knowledge obtained in the program from MS Intelligence and cybersecurity courses using analytic tradecraft standards and cybersecurity tools to undertake a comprehensive research project that addresses a real, substantive cybersecurity related problem.	All Program courses	PSCI 699: MS Culminating Project
PLO 3. Problem solving with Information Systems Technology: Each graduate student will apply IST knowledge in new and unfamiliar circumstances and devise innovative solutions to solve business problems and cope with unforeseen events including analyzing IST organizational needs, designing and implementing secure IST applications, cyber defense/offence, risk management, securing networks, and cybercrime investigation and litigation.	SLO3. The graduate student shall understand and apply appropriate research methods and structured analytic techniques to identify, collect, analyze, and transform data into accurate information for presentation to policy makers and other target stakeholders.	PSCI 592:Seminar in Government PSCI 590: Techniques of Intelligence Analysis PSCI 621: Strategic Intelligence PSCI 600: Theory and History of Strategy	PSCI 699 or PSCI 999
	SLO4. The graduate student shall understand, select, and apply appropriate technologies, policies, and procedures (including forensic tools) needed to assure the confidentiality, integrity, and availability of information systems.	IST 525: Computer Forensics IST 610: Information Assurance, Policy and Management IST 609: Information Systems and Technology Management IST 511: Cyber Defense	
	SLO5. The graduate student shall understand business models and identify a business (IST) problem, analyze (IST requirements, and apply secure design principles used in information systems development and implementation projects.	IST 609: Information Systems and Technology Management IST 647: Information Based Management IST 646: Systems Planning, Strategy and Policy	
	SLO6. The graduate student shall understand enterprise information systems and technology architectures and the IST governance processes.	IST 646: Systems Planning, Strategy and Policy	
PLO 4. Ethical Reasoning in a Global Context: Each student will identify, evaluate and discuss ethical and regulatory cybersecurity issues at an individual, professional, organizational, local, state, national and global context.	SLO7. The graduate student shall understand and integrate the legal, ethical, and global implications of IST as it relates to Cybersecurity, Cyber Warfare, and Strategic Systems	PSCI 601: Strategic Systems and Thought PSCI 621: Strategic Intelligence PSCI 484: National Security Policy PSCI 603: Cybersecurity and Cyber Warfare	PSCI 699 or PSCI 999

Table 3:
Summary Matrix showing where student learning outcomes are introduced (I), developed (D) and mastered (M)

	PSCI 484	PSCI 590	PSCI 592	PSCI 600	PSCI 601	PSCI 603	PSCI 621	IST 511	IST 609	IST 610	IST 646	IST 525	IST 647	PSCI 999	PSCI 699
SLO1.	I/D	D	I/D	D	D	D	D/M	I/D	D	D	D	D	D		M
SLO2	I/D	D	I/D	D	D	D	D	I/D	I/D	I/D	I/D	D	I/D	M	
SLO3	I	I/D	I/D	I/D			D							M	M
SLO4								I/D	D	I/D		I/D		M	M
SLO5									D		D		I/D	M	M
SLO6											I/D			M	M
SLO7	I/D				I/D	D	D							M	M

Table XX: Summary of Direct Assessment Measures:

Outcomes	Class	Method
Specific Knowledge and Skills	PSCI 699 PSCI 999	Culminating Applied Project Culminating Comprehensive Exam
Communication	PSCI 699 PSCI 999	Culminating Applied Project Presentation Culminating Comprehensive Exam Presentation
Problem Solving with Information Technology	PSCI 699 PSCI 999	Culminating Applied Project Culminating Comprehensive Exam
Ethical Reasoning in a Global Context	PSCI 699 PSCI 999	Culminating Applied Project Culminating Comprehensive Exam

Indirect assessment measures:

- Bi-annual Assurance of Learning Reports and Faculty Forums
- Bi-annual CIR Reports
- Syllabus Analysis
- Internship Survey
- Employer Survey
- Student Survey
- Assessment Center

5. Additional Insights on Lessons Learned

We reserved the best for the last. We have found the home and school learning environments, pre-established alumni mentor relationships, team work, and alignment of personal vision with service critical factors for student success.

1. **Home learning environment**
   The student home support infrastructure includes parents, siblings, and friends. During the student screening interview, especially Scholarship for Service applicants, we request students to bring either a parent, sibling or loved one. We explain to them the expectations we have for the student and specifically, the type of support expected at home. We make clear the onerous responsibilities we will put on the student and the kind of support the student needs to succeed. No contract is signed, but this becomes a binding verbal contract.
2. **School Learning Environment**
   Cybersecurity Intelligence students are expected to become members of the InfoSec club. Here students learn the meaning of team work and there is no shame in admitting you cannot know everything. Club activities include learning from each other through a paired mentor—mentee relationship; working on individual and assigned projects; community activities in elementary, junior, and high schools, preparing for cyber challenge competitions, and CyberGen activities. And of course attending classes, attending the industry speaker series presentations, preparing and passing industry certifications, de-briefings, and making assigned presentations.

3. **Future Work Environment**

The support and feedback students get from former working students is invaluable. Students are able to see the light at the end of the tunnel and truly confirm why their effort is just worth it. They are also able to re-assess their interests and affirm their calling to service. On occasion we have former students making a presentation to the InfoSec club, or teach a class for us.

4. **Alignment of personal Vision, Country and Service**
   Again during the pre-screening interview, ask the student to share with us her/his personal vision, involvement with community service, and how that aligns with the quest for serving the nation. We find the alignment of personal vision and goals is critical for student and program success.

5. **Recruitment and Articulation with Community Colleges**
   In order to ensure diversity of the pool of the students we draw from, we have articulated with several community colleges (CCs). Students from the CCs join our program as juniors, most of them taking advantage of the SFS grants. This has enriched our program with capable and talented under-represented students.

Appendix 1: Model Curriculum for Cyber Security and Intelligence Analysis

For the Intelligence Analysis component of the curriculum, we have discovered an interesting problem. The required competencies for cyber and intelligence are different for each discipline. For cyber, the NICE Cybersecurity Workforce Framework (NCWF) (November 2016)[4] spells out the required Knowledge, Skills, and Abilities (KSAs). Very little of such KSAs reflect the analytic competencies of the intelligence community. While two workforce categories include two (2) areas that would seem to overlap with intelligence (AN-Analyze; and CO-Collect and Operate), the KSAs that have remote relationship to intelligence analysis are low. Knowledge (K) has only 2.8% clearly related; Skills (S) has about 15% clearly related; and Abilities (A) has about 26% clearly related to intelligence analysis.

The source for intelligence competencies is found in the Office of the Director of National Intelligence's (ODNI) Intelligence Community Directive (203) (ICD 2003, January 2015)[5]. These competencies set the "Intelligence Community Analytic Standards" for the entire Intelligence Community (IC) workforce.

The ODNI's IDC 203 directs the intelligence community as a workforce to exemplify the following five (5) Analytic Standards. Overall, analysts are to be:

1) Objective: awareness of own assumptions and reasoning
2) Independent of political considerations
3) Timely
4) Based on all available sources of intelligence
5) Exhibits analytic tradecraft standards (see below)

IDC 203 also specified nine (9) specific Analytic Tradecraft Standards to fulfill standard 5) above:

1) Describes quality and credibility of underlying sources, data, and methodologies
2) Expresses and explains uncertainties associated with analytic judgments
3) Distinguishes between underlying intelligence information and analysts' assumptions and judgments
4) Incorporates analysis of alternatives
5) Demonstrates customer relevance and addresses implications
6) Uses clear and logical argumentation
7) Explains change to or consistency of analytic judgments
8) Makes accurate judgments and assessments
9) Incorporates effective visual information where appropriate

[4] Commerce, Department of, NIST Special Publication 800-181: NICE Cybersecurity Workforce Framework (NCWF), (November 2016), http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-181. (Draft; open for comment.)
[5] Office of the Director of National Intelligence (ODNI), Intelligence Community Directive 203, Intelligence Community Analytic Standards (2 January 2015), https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

But IC workforce competencies are not required for entry-level analysts. As these standards refer to the workforce of the IC, they do not indicate how to prepare students for intelligence careers. Therefore, NSS faculty conducted a study (November 2016) of 14 representative samples from entry-level positions across a number of intelligence agencies.

These agency postings for entry level positions, or entry-level positions requiring intelligence skills, including Air Force Intelligence, Army Intelligence, the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the Department of Homeland Security (DHS), the Department of Energy (DOE), the Drug Enforcement Administration (DEA), the Department of State, the Federal Bureau of Investigation (FBI), the National Counterterrorism Center (NCTC), the National Geospatial Intelligence Agency (NGA), the National Security Agency (NSA), the U.S. Marine Corps Intelligence Activity and a non-IC agency, the Government Accountability Office (GAO). Their overall requirements and frequency are listed below. A second study of eight (8) specific cyber intelligence analyst job postings researched in April 2017 from the following agencies reflected the same emphasis for the social science side, including the Central Intelligence Agency, the Department of Defense, the Department of Homeland Security, the Federal Bureau of Investigation, the Office of the Director of National Intelligence, the National Security Agency, the U.S. Coast Guard, and the U.S. Air Force:

Code	**General/Common Skills**	**% Agencies requiring**
CW	Clear Writing	100%
OC	Clear oral communication	95%
AD	Analyze data/information	95%
AE	Analyze alternative explanations	80%
IG	Identify information gaps	40%
TW	Team work/collaboration	30%
RG	Regional/Geographic knowledge	30%
LG	Language skills (preferred, not required)	30%

Model Curriculum for Intelligence (BS, MS)

Bachelor of Science

The courses listed below are "core" courses for every student specializing in intelligence analysis as part of the B.S. emphasis on Cyber Security, Intelligence concentration. While this degree is housed in the College of Business and Public Administration, our contribution is designed to familiarize such students with basic levels of politics and policy as it relates to intelligence analysis. We believe the content and competencies can be addressed by a variety of different courses, so these are illustrative only. The goal here is to encourage people from a business school perspective to gain understanding of national and international security and introduce them to intelligence analysis. The content and competencies we addressed are included as well, especially as they pertain to hiring for intelligence analysis.

Topic	Content/Competencies	Codes addressed
American Foreign Policy	Content: Introduction to the institutions and bureaucracies charged with U.S. foreign policy. Competencies: writing for policy, introduction to analysis, oral presentation.	CW, OC, AD, RG
International Relations Theories	Content: Introduction and overview of theories of international politics. Competencies: understanding theory and the role of assumptions in theoretical thinking, writing, oral presentation.	CW, OC, AD, AE
National Security Policy	Content: Introduction to National Security, institutions, strategy and policies. Competencies: Intelligence Cycle, writing for policy, oral presentation.	CW, OC, AD, RG
Techniques of Intelligence Analysis	Content and competencies: Introduction to Structured Analytical Techniques[6] --Analysis of Competing Hypotheses --Structured Brainstorming --Red Teaming --Argument Mapping --Key Assumptions Check Writing for intelligence, oral presentation.	CW, OC, AD, AE, IG, TW

[6] Richards J. Heuer and Randolf H. Pherson, Structured Analytical Techniques for Intelligence Analysis, 2nd Edition (Washington, D.C.: CQ Press, 2015).

Master of Science, National Cyber Security Studies

The courses listed below are "core" courses for every student studying cyber security and intelligence at the M.S. level. Students that have taken one or more of these courses as undergraduates are in the position of being able to take additional "elective" classes that would emphasize a regional (Middle East, East Asia, Africa, Eurasia) or functional (Terrorism) concentration or perhaps add additional courses in intelligence (Intelligence Ethics, Intelligence Failures) or national security (Arms Control, International Law, International Security). The content and competencies we addressed are included as well, especially as they pertain to hiring for intelligence analysis.

Topic	**Content/Competencies**	**Codes addressed**
National Security Policy	Content: Introduction to National Security, institutions, strategy and policies. Competencies: Intelligence Cycle, writing for policy, oral presentation.	CW, OC, AD, RG
Techniques of Intelligence Analysis	Content and competencies: Introduction to Structured Analytical Techniques[7] --Analysis of Competing Hypotheses --Structured Brainstorming --Red Teaming --Argument Mapping --Key Assumptions Check Writing for intelligence, oral presentation.	CW, OC, AD, AE, IG, TW
Research Methods	Content: Research Methods, Scientific Revolutions, Logic and Fallacies, difference between correlation and causation.	CW, OC, AD, AE, IG, TW
Theory and History of Strategy	Content: Major authors/works of strategy and war Writing[8] (multiple short essays) --Different audiences --Coherence --Cohesion --Clarity --Concision Analysis (8 elements of reasoning)[9] --Purpose	CW, OC, AD, AE, IG

[7] Richards J. Heuer and Randolf H. Pherson, Structured Analytical Techniques for Intelligence Analysis, 2nd Edition (Washington, D.C.: CQ Press, 2015).
[8] Joseph M. Williams and Joseph Bizup, Style: Writing for Clarity and Grace, 12th Edition (Pearson, 2014).
[9] Linda Elder and Richard Paul, The Thinker's Guide to Analytical Thinking, (Foundation for Critical Thinking, 2010), www.criticalthinking.org.

	--Question --Information and data --Inference and interpretation --Concepts and ideas --Assumptions --Implications --Point of View	
Strategic Systems and Thought	Content: weapons of mass destruction Re-introduce basic analysis (8 elements of reasoning) --Purpose --Question --Information and data --Inference and interpretation --Concepts and ideas --Assumptions --Implications --Point of View Writing (longer essay) --Different audiences --Coherence --Cohesion --Clarity --Concision	CW, OC, AD, AE, IG, RG
Cyber Security and Cyber Warfare	Content: policies and problems with cyber security and cyber warfare. Reasoning and writing (longer essays on a substantive topic of cyber security or cyber warfare).	CW, OC, AD, AE, IG, TW
Strategic Intelligence	Content: Individual and group strategic assessment of a security issue. Group effort to practice negotiating differences and reaching consensus. More Structured Analytic Techniques. Presentations to class, and to wider faculty/student audiences.	CW, OC, AD, AE, IG, TW

For language training, we encourage students to apply for scholarships for language study, which is outside the curriculum. For both degrees, there are other things that recruiters look for that are not listed on the job announcements, but weigh in favor of the student. However, they are not typically part of the curriculum either, as the recruiters like to see student involvement in activities outside the classroom. Such activities include: presentation of papers at conferences, involvement in student government or student clubs, work experience that may relate to the job announcement (such as managerial experience), and the like. As they are not part of the curriculum, we encourage students to become involved in these activities where practicable. As well, we encourage students to learn how to write resumes and learn how to interview better, which Career Services for Students provide.