MEMORANDUM OF AGREEMENT

between

University of Pittsburgh
Department of Information Sciences and Telecommunications
Pittsburgh, Pennsylvania
and
National Defense University
Information Resources Management College
Washington, D.C.

University of Pittsburgh, hereafter referred to as Pitt, and the National Defense University's Information Resources Management College, hereafter referred to as "NDU/IRMC," agree to a joint mission to provide extended academic opportunities to their respective students and faculty. It is understood that the goals of the joint mission include:

- Strengthening the quality and breadth of academic programs at both institutions.
- Promoting an educational environment where faculty and graduate students from both institutions can learn from one another through sharing of information and knowledge.
- Leveraging the strengths and resources of programs at both institutions.

Within Pitt, the Department of Information Science and Telecommunications (DIST) (with an Information Assurance (IA) emphasis), within the School of Information Sciences (SIS) is interested in accepting DoD students into its graduate programs. Pitt is willing to award **15 graduate credit hours** of advanced standing for students who complete the Chief Information Officer (CIO) Certificate Program or Advanced Management Program (AMP) with IA emphasis and **9 graduate credit hours** of advanced standing for students who complete the IA Certificate from NDU/IRMC. The following degrees may be awarded from the SIS: Master of Science in Information Science (MSIS) or Master of Science in Telecommunications and Networking (MST&N), after IRMC CIO/AMP certificate (with IA emphasis) holders have completed an additional 21 credit hours of graduate credit work, or IRMC IA certificate holders have completed an additional 27 credit hours of graduate credit at SIS.

Prerequisites for DoD students are the same as those for all transfer students to SIS, including an overall grade point average of B or better. Curriculum content of graduate programs proposed for the DoD students is defined by the department issuing the degree and is dependent on the options selected by the student.

Whereas the above named institution(s) recognize that a Memorandum of Understanding would be of mutual benefit and would serve as an indication of intent to cooperate as a means of achieving the mission, it is understood that:

1. Each institution meets the qualifications needed to satisfy the conditions set forth by the Department of Defense Information Assurance Scholarship Program (IASP) solicitation including:

   o Accreditation by the Association of Colleges and Schools, and

      o Certification by the U.S. National Security Agency as a Center of Academic Excellence (CAE) in Information Assurance and Security.

2. Each institution will provide an interface of graduate programs, thereby serving to enhance educational synergy which will significantly impact effectiveness in information assurance education.

3. Each institution agrees that each NDU/IRMC student enrolled at SIS under the partnership program will be subject to all SIS rules and policies governing the degree award, including maintenance of satisfactory performance, and completion of the remaining credit hours inherent to the student's specific degree program.

4. Each institution will announce and promote this collaboration and demonstrate their best efforts to ensure a successful partnership program.

5. This Memorandum of Understanding will be effective from the date of signing and will have a duration of three years. Upon expiration of the three years, the MOU will be subject to renewal. Additions and changes to this MOU may be made at any time with the written agreement of both SIS and NDU/IRMC. Either SIS or NDU/IRMC may withdraw from this Agreement upon 60 days written notice to the other institution made to the institutional contact address, via U.S. Certified mail.

The following persons will serve as Points of Contact at SIS and NDU/IRMC:

Dr. James B D Joshi, Assistant Professor
Department of Information Science and Telecommunications
University of Pittsburgh
135 North Bellefield Avenue
Pittsburgh PA 15260
Phone: (412) 624-9982
Fax: (412) 624-2788
jjoshi@mail.sis.pitt.edu

Ms. Mary Polydys
Dept. of Information Operations and Assurance Chair
National Defense University
Information Resources Management College
Fort Lesley J. McNair, Marshall Hall
Washington, DC 20319-5066
Phone (202) 685-3889
Fax (202) 685-3974
polydysm@ndu.edu

The undersigned agree to the provisions as outlined above in the Memorandum of Understanding and state that they have the authority to bind their respective institution to this Agreement.
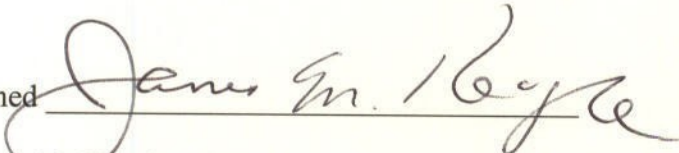
Signed _Ronald L Larsen_   Date_8-11-05_

Ronald L. Larsen, PhD
Dean and Professor, SIS
University of Pittsburgh
Pittsburgh, PA

Signed _James V. Maher_   Date_10/7/05_

James V. Maher, PhD
Provost and Senior Vice Chancellor
University of Pittsburgh
Pittsburgh, PA

Signed _James M. Keagle_   Date_15 Sep 05_

James M. Keagle, PhD
Provost and Vice President for Academic Affairs
National Defense University
Washington, DC

Annex A:	**Overview of NDU/IRMC IA, CIO and AMP Certificate Programs**
Annex B:	**Transfer of Courses and Course Requirements at DIST for NDU/IRMC IA, CIO and AMP Certificate Students**
Annex C:	**Overview of Committee on National Security Systems (CNSS) standards**

Annex A – Overview of NDU/IRMC IA, CIO and AMP Certificate Programs

NOTE: The following information reflects IRMC programs for the 2004-2005 academic year. IRMC reserves the right to change course names, abbreviations, or content to continue to meet the CIO, AMP, or IA requirements.

Information Assurance Certificate

The **IA Certificate Program** consists of a series of courses that emphasize security issues and approaches fundamental to the protection of the information infrastructure. The Committee on National Security Systems (CNSS) has certified the curriculum offered by the Information Resources Management (IRM) College as being compliant with CNSS No. 4011 Standard for Information Systems Security Professionals and CNSS No. 4012, the standard for Senior System Managers.

The primary teaching method of resident and distributed courses is the seminar, supplemented by guest speakers. This requires interaction and engagement by all participants in discussions, and individual and collaborative exercises.

The IA 4011 certification requires students to complete a series of four courses offered in residence, through distributed learning format via the web or through a combination of these formats. Students must successfully complete the academic requirements of these courses to receive 4011 certification:

      C1.   Information Assurance and Critical Infrastructure Protection (AII);
      C2   Global Enterprise Networking and Telecommunications (GEN);
      C3   Managing Information Security in a Networked Environment (SEC); and
      C4   Developing Enterprise Security Strategies, Guidelines, and Policy (ESS).

A fifth course, C5, Approval to Operate: Information Systems Certification and Accreditation (ATO), can be completed by IRMC students to earn the 4012 certification as well.

It is strongly recommended that the first two courses be AII and GEN, followed by SEC, and finally ESS. Successful completion of this option results in 4011 certification. Completion of three of these four courses may be applied toward requirements for the CIO Certificate Program. Completion of the ATO course results in 4012 certification. Students in the Advanced Management Program also have the opportunity to qualify for the certification.

Chief Information Officer & Advanced Management Program (with IA Emphasis)

Award of the CIO Certificate requires successful completion of eight intensive courses OR the Advanced Management Program (AMP) OR a combination of eight intensive and elective courses. Six courses must be primary courses in different subject areas; the remaining two courses may be either primary or enrichment courses in any subject area. Primary courses in Policy and Performance and Results-Based Management subject areas are mandatory courses for everyone. Students may opt to complete the CIO Certificate with an IA concentration leading to the IA 4011 Certificate. This concentration requires four IA Certificate courses (course C1 through C4 listed above). This option requires completion of nine courses instead of eight. AII counts as a primary course; SEC, GEN, and ESS count as enrichment courses.

The AMP is a fourteen-week educational program that provides mid-level and senior leaders with an integrated graduate-level education focused on the policies and imperatives that enable federal national security and civilian agencies to leverage information for strategic advantage. It has three elements that define its unique educational experience. First, the AMP has both core and elective courses that provide a foundation of skills and knowledge in a broad range of information resources management disciplines. All AMP students earn a CIO Certificate. AMP students focusing on IA may complete at least three of the four courses required for an IA 4011 Certificate.

Annex B – Course Requirements at DIST for NDU/IRMC IA, CIO and AMP Students

The course requirements for the SAIS track students within the MSIS and MST programs are as shown in figures 1 and 2.
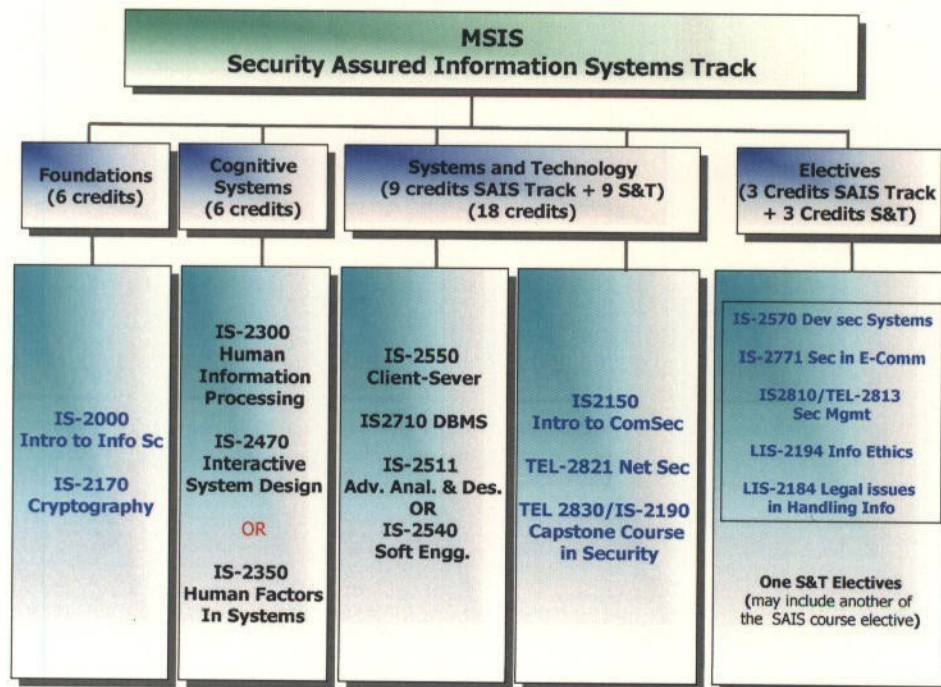

Figure 1. Requirements for SAIS students in MSIS program at DIST

The MSIS-SAIS students are required to fulfill the area requirements (6 credits Foundations, 6 credits Cognitive systems, 18 credits Systems and Technologies and 6 credits Electives), as indicated in Figure 1. The courses shown are highly recommended for the SAIS track and special permission is needed to replace indicated course by another MSIS courses (not listed here). Similarly, the MST-SAIS track requirements are detailed in Figure 2.

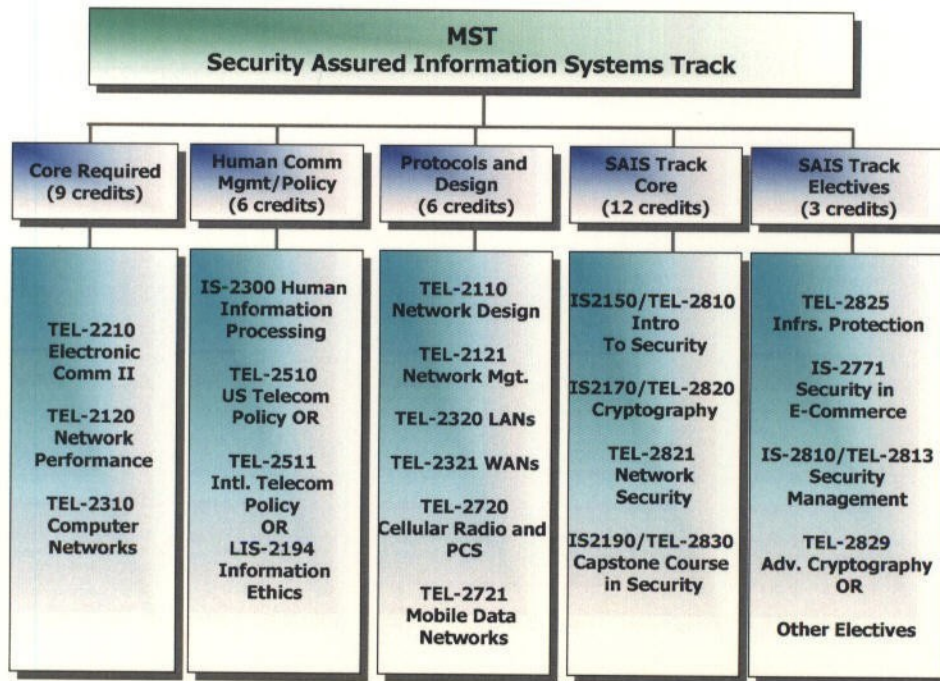| MST Security Assured Information Systems Track				
Core Required (9 credits)	Human Comm Mgmt/Policy (6 credits)	Protocols and Design (6 credits)	SAIS Track Core (12 credits)	SAIS Track Electives (3 credits)
TEL-2210 Electronic Comm II TEL-2120 Network Performance TEL-2310 Computer Networks	IS-2300 Human Information Processing TEL-2510 US Telecom Policy OR TEL-2511 Intl. Telecom Policy OR LIS-2194 Information Ethics	TEL-2110 Network Design TEL-2121 Network Mgt. TEL-2320 LANs TEL-2321 WANs TEL-2720 Cellular Radio and PCS TEL-2721 Mobile Data Networks	IS2150/TEL-2810 Intro To Security IS2170/TEL-2820 Cryptography TEL-2821 Network Security IS2190/TEL-2830 Capstone Course in Security	TEL-2825 Infrs. Protection IS-2771 Security in E-Commerce IS-2810/TEL-2813 Security Management TEL-2829 Adv. Cryptography OR Other Electives

Figure 2. Requirements for SAIS students in MST program at DIST

Noting the difference in the structure and content coverage between the DIST's SAIS curriculum and that of the IRMC certificate programs, primarily because of the NDU/IRMC's strong focus on the requirements of the federal IT systems and infrastructures, the DIST will give 9 credits of advanced standing to NDU/IRMC IA certificate students for the following courses:

- IS2150/TEL2810 Introduction to Computer Security
- IS2810/TEL2813 Security Management
- One Elective (One S&T Elective for MSIS, One Policy elective for MST)

This advanced placement is based on the coverage of the IA certificate courses C1 through C4 which closely matches the coverage of IS2150 and IS2810. Additionally, the courses C1 through C4 also covers substantial material focused on security and IT issues related to federal systems that are not addressed by the SAIS curriculum. Hence, the transfer student will be considered to have completed an elective within the S&T pool for MSIS-SAIS track and for the Policy pool for the MST-SAIS track.

The NDU/IRMC CIO/AMP certificate students with IA focus will be given 15 credits of advanced placement, 9 credits of which would be that applied to the IA certificate as shown above. Remaining 6 credits of advanced placement will be given for the following courses:

- IS2190/TEL2830 Capstone Requirement
- IS2000 Introduction to Information Science for MSIS, or one Human/Mgmt area requirement for MST

The SAIS capstone requirement is tailored towards facilitating students to develop skills in a particular practical IA issue. The CIO/AMP certificate course requirements significantly focus on the IA issues related to the federal systems and infrastructure and hence will be considered as having fulfilled a capstone requirement. IS2000 covers broad, current issues related to information sciences, which are addressed in the CIO/AMP courses.

Note that once the IRMC certificate holders complete the remaining requirements after transferring to DIST, they are eligible for all the five CNSS standards (CNSS 4011 to 4015). The SAIS curriculum requirements are more rigorous than the general MSIS degree requirements (although admissions requirements are essentially the same) and the SAIS students may have to take more courses than shown above.

Annex C – Overview of the Committee of National Systems Security (CNSS) standards

Pitt's SAIS curriculum has been certified for the CNSS standards 4011, 4012, 4013, 4014A and 4015. NDU/IRMC's IA curriculum has been certified for CNSS 4011 and 4012.

CNSS 4011 - NATIONAL TRAINING STANDARD FOR INFORMATION SYSTEMS SECURITY (INFOSEC) PROFESSIONALS:

This instruction provides the minimum course content for the training of information systems security (INFOSEC) professionals in the disciplines of telecommunications security and automated information systems (AIS) security.

CNSS 4012- NATIONAL TRAINING STANDARD FOR DESIGNATED APPROVING AUTHORITY (DAA)

This instruction establishes the minimum course content or standard for the development and implementation of training for Designated Approving Authorities in the disciplines of telecommunications security and information systems (IS) security.

CNSS 4013 - NATIONAL TRAINING STANDARD FOR SYSTEM ADMINISTRATORS IN INFORMATION SYSTEMS SECURITY (INFOSEC)

This instruction establishes the minimum course content or standard for the development and implementation of training for system administrator professionals in the disciplines of telecommunications security and information systems (IS) security.

CNSS 4014 - NATIONAL TRAINING STANDARD FOR INFORMATION SYSTEMS SECURITY OFFICERS (Advanced level)

This instruction establishes the minimum course content or standard for the development and implementation of training for Information Systems Security Officers (ISSO) in the disciplines of telecommunications security and information systems (IS) security. Please check with your agency for applicable implementing documents.

CNSS 4015 - NATIONAL TRAINING STANDARD FOR SYSTEM CERTIFIERS

This instruction establishes the minimum course content or standard for the development and implementation of education and training for System Certifier professionals in the disciplines of telecommunications security and information systems (IS) security. Please check with your agency for applicable implementing documents.

For more information on the CNSS standards, see:
http://www.nsa.gov/ia/academia/cnsstesstandards.cfm

University of Pittsburgh

August 11, 2005

Patricia Coopersmith
National Defense University, IRMC
Fort Lesley J. McNair, Marshall Hall
Washington, DC   20319-5066

Dear Ms. Coopersmith:

Hi! I understand from Dr. James Joshi that you are expecting the enclosed copies of the Memorandum of Agreement between the University of Pittsburgh's Department of Information Science and Telecommunications and the National Defense University's Information Resources Management College. Please find enclosed two (2) copies.

We would appreciate your asking Dr. Keagle to review and sign both copies. Then, please return both copies to us. We will have our Provost sign (he is currently traveling) and will send one of the originals back to you.

If you have any questions, please give me a call on 412/624-5139.

Thank you.

Carolyn M. Loether

Carolyn M. Loether
Assistant to Dean Larsen

URGM&P 33587

MEMORANDUM OF AGREEMENT

between

University of Pittsburgh
Department of Information Sciences and Telecommunications
Pittsburgh, Pennsylvania
and
National Defense University
Information Resources Management College
Washington, D.C.

University of Pittsburgh, hereafter referred to as Pitt, and the National Defense University's Information Resources Management College, hereafter referred to as "NDU/IRMC," agree to a joint mission to provide extended academic opportunities to their respective students and faculty. It is understood that the goals of the joint mission include:

- Strengthening the quality and breadth of academic programs at both institutions.
- Promoting an educational environment where faculty and graduate students from both institutions can learn from one another through sharing of information and knowledge.
- Leveraging the strengths and resources of programs at both institutions.

Within Pitt, the Department of Information Science and Telecommunications (DIST) (with an Information Assurance (IA) emphasis), within the School of Information Sciences (SIS) is interested in accepting DoD students into its graduate programs. Pitt is willing to award **15 graduate credit hours** of advanced standing for students who complete the Chief Information Officer (CIO) Certificate Program or Advanced Management Program (AMP) with IA emphasis and **9 graduate credit hours** of advanced standing for students who complete the IA Certificate from NDU/IRMC. The following degrees may be awarded from the SIS: Master of Science in Information Science (MSIS) or Master of Science in Telecommunications and Networking (MST&N), after IRMC CIO/AMP certificate (with IA emphasis) holders have completed an additional 21 credit hours of graduate credit work, or IRMC IA certificate holders have completed an additional 27 credit hours of graduate credit at SIS.

Prerequisites for DoD students are the same as those for all transfer students to SIS, including an overall grade point average of B or better. Curriculum content of graduate programs proposed for the DoD students is defined by the department issuing the degree and is dependent on the options selected by the student.

Whereas the above named institution(s) recognize that a Memorandum of Understanding would be of mutual benefit and would serve as an indication of intent to cooperate as a means of achieving the mission, it is understood that:

1. Each institution meets the qualifications needed to satisfy the conditions set forth by the Department of Defense Information Assurance Scholarship Program (IASP) solicitation including:
   o Accreditation by the Association of Colleges and Schools, and

1

- o Certification by the U.S. National Security Agency as a Center of Academic Excellence (CAE) in Information Assurance and Security.
2. Each institution will provide an interface of graduate programs, thereby serving to enhance educational synergy which will significantly impact effectiveness in information assurance education.
3. Each institution agrees that each NDU/IRMC student enrolled at SIS under the partnership program will be subject to all SIS rules and policies governing the degree award, including maintenance of satisfactory performance, and completion of the remaining credit hours inherent to the student's specific degree program.
4. Each institution will announce and promote this collaboration and demonstrate their best efforts to ensure a successful partnership program.
5. This Memorandum of Understanding will be effective from the date of signing and will have a duration of three years. Upon expiration of the three years, the MOU will be subject to renewal. Additions and changes to this MOU may be made at any time with the written agreement of both SIS and NDU/IRMC. Either SIS or NDU/IRMC may withdraw from this Agreement upon 60 days written notice to the other institution made to the institutional contact address, via U.S. Certified mail.

The following persons will serve as Points of Contact at SIS and NDU/IRMC:

Dr. James B D Joshi, Assistant Professor
Department of Information Science and Telecommunications
University of Pittsburgh
135 North Bellefield Avenue
Pittsburgh PA 15260
Phone: (412) 624-9982
Fax: (412) 624-2788
jjoshi@mail.sis.pitt.edu

Ms. Mary Polydys
Dept. of Information Operations and Assurance Chair
National Defense University
Information Resources Management College
Fort Lesley J. McNair, Marshall Hall
Washington, DC 20319-5066
Phone (202) 685-3889
Fax (202) 685-3974
polydysm@ndu.edu

The undersigned agree to the provisions as outlined above in the Memorandum of Understanding and state that they have the authority to bind their respective institution to this Agreement.

Signed _____   Date 8-11-05

Ronald L. Larsen, PhD
Dean and Professor, SIS
University of Pittsburgh
Pittsburgh, PA

Signed _____   Date 10/7/05

James V. Maher, PhD
Provost and Senior Vice Chancellor
University of Pittsburgh
Pittsburgh, PA

Signed _____   Date 5 Sep 05

James M. Keagle, PhD
Provost and Vice President for Academic Affairs
National Defense University
Washington, DC

Annex A: **Overview of NDU/IRMC IA, CIO and AMP Certificate Programs**
Annex B: **Transfer of Courses and Course Requirements at DIST for NDU/IRMC IA, CIO and AMP Certificate Students**
Annex C: **Overview of Committee on National Security Systems (CNSS) standards**

Annex A – Overview of NDU/IRMC IA, CIO and AMP Certificate Programs

NOTE: The following information reflects IRMC programs for the 2004-2005 academic year. IRMC reserves the right to change course names, abbreviations, or content to continue to meet the CIO, AMP, or IA requirements.

Information Assurance Certificate

The **IA Certificate Program** consists of a series of courses that emphasize security issues and approaches fundamental to the protection of the information infrastructure. The Committee on National Security Systems (CNSS) has certified the curriculum offered by the Information Resources Management (IRM) College as being compliant with CNSS No. 4011 Standard for Information Systems Security Professionals and CNSS No. 4012, the standard for Senior System Managers.

The primary teaching method of resident and distributed courses is the seminar, supplemented by guest speakers. This requires interaction and engagement by all participants in discussions, and individual and collaborative exercises.

The IA 4011 certification requires students to complete a series of four courses offered in residence, through distributed learning format via the web or through a combination of these formats. Students must successfully complete the academic requirements of these courses to receive 4011 certification:
   C1.   Information Assurance and Critical Infrastructure Protection (AII);
   C2   Global Enterprise Networking and Telecommunications (GEN);
   C3   Managing Information Security in a Networked Environment (SEC); and
   C4   Developing Enterprise Security Strategies, Guidelines, and Policy (ESS).
A fifth course, C5, Approval to Operate: Information Systems Certification and Accreditation (ATO), can be completed by IRMC students to earn the 4012 certification as well.

It is strongly recommended that the first two courses be AIIand GEN, followed by SEC, and finally ESS. Successful completion of this option results in 4011 certification. Completion of three of these four courses may be applied toward requirements for the CIO Certificate Program. Completion of the ATO course results in 4012 certification. Students in the Advanced Management Program also have the opportunity to qualify for the certification.

Chief Information Officer & Advanced Management Program (with IA Emphasis)

Award of the CIO Certificate requires successful completion of eight intensive courses OR the Advanced Management Program (AMP) OR a combination of eight intensive and elective courses. Six courses must be primary courses in different subject areas; the remaining two courses may be either primary or enrichment courses in any subject area. Primary courses in Policy and Performance and Results-Based Management subject areas are mandatory courses for everyone. Students may opt to complete the CIO Certificate with an IA concentration leading to the IA 4011 Certificate. This concentration requires four IA Certificate courses (course C1 through C4 listed above). This option requires completion of nine courses instead of eight. AII counts as a primary course; SEC, GEN, and ESS count as enrichment courses.

The AMP is a fourteen-week educational program that provides mid-level and senior leaders with an integrated graduate-level education focused on the policies and imperatives that enable federal national security and civilian agencies to leverage information for strategic advantage. It has three elements that define its unique educational experience. First, the AMP has both core and elective courses that provide a foundation of skills and knowledge in a broad range of information resources management disciplines. All AMP students earn a CIO Certificate. AMP students focusing on IA may complete at least three of the four courses required for an IA 4011 Certificate.

Annex B – Course Requirements at DIST for NDU/IRMC IA, CIO and AMP Students

The course requirements for the SAIS track students within the MSIS and MST programs are as shown in figures 1 and 2.
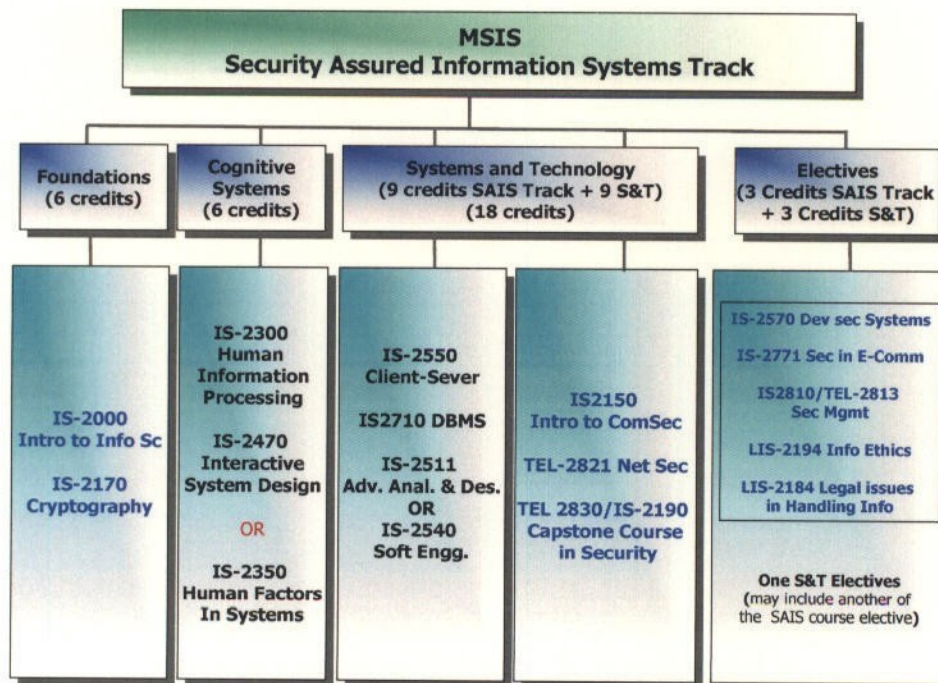

Figure 1. Requirements for SAIS students in MSIS program at DIST

The MSIS-SAIS students are required to fulfill the area requirements (6 credits Foundations, 6 credits Cognitive systems, 18 credits Systems and Technologies and 6 credits Electives), as indicated in Figure 1. The courses shown are highly recommended for the SAIS track and special permission is needed to replace indicated course by another MSIS courses (not listed here). Similarly, the MST-SAIS track requirements are detailed in Figure 2.

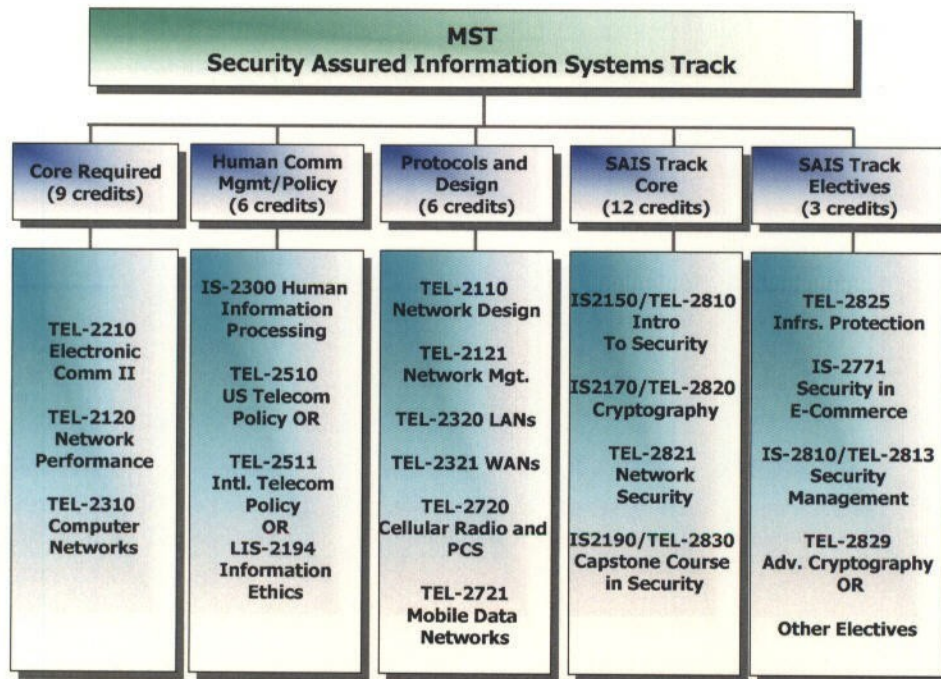| MST Security Assured Information Systems Track				
Core Required (9 credits)	Human Comm Mgmt/Policy (6 credits)	Protocols and Design (6 credits)	SAIS Track Core (12 credits)	SAIS Track Electives (3 credits)
TEL-2210 Electronic Comm II TEL-2120 Network Performance TEL-2310 Computer Networks	IS-2300 Human Information Processing TEL-2510 US Telecom Policy OR TEL-2511 Intl. Telecom Policy OR LIS-2194 Information Ethics	TEL-2110 Network Design TEL-2121 Network Mgt. TEL-2320 LANs TEL-2321 WANs TEL-2720 Cellular Radio and PCS TEL-2721 Mobile Data Networks	IS2150/TEL-2810 Intro To Security IS2170/TEL-2820 Cryptography TEL-2821 Network Security IS2190/TEL-2830 Capstone Course in Security	TEL-2825 Infrs. Protection IS-2771 Security in E-Commerce IS-2810/TEL-2813 Security Management TEL-2829 Adv. Cryptography OR Other Electives

Figure 2. Requirements for SAIS students in MST program at DIST

Noting the difference in the structure and content coverage between the DIST's SAIS curriculum and that of the IRMC certificate programs, primarily because of the NDU/IRMC's strong focus on the requirements of the federal IT systems and infrastructures, the DIST will give 9 credits of advanced standing to NDU/IRMC IA certificate students for the following courses:

- IS2150/TEL2810 Introduction to Computer Security
- IS2810/TEL2813 Security Management
- One Elective (One S&T Elective for MSIS, One Policy elective for MST)

This advanced placement is based on the coverage of the IA certificate courses C1 through C4 which closely matches the coverage of IS2150 and IS2810. Additionally, the courses C1 through C4 also covers substantial material focused on security and IT issues related to federal systems that are not addressed by the SAIS curriculum. Hence, the transfer student will be considered to have completed an elective within the S&T pool for MSIS-SAIS track and for the Policy pool for the MST-SAIS track.

The NDU/IRMC CIO/AMP certificate students with IA focus will be given 15 credits of advanced placement, 9 credits of which would be that applied to the IA certificate as shown above. Remaining 6 credits of advanced placement will be given for the following courses:

- IS2190/TEL2830 Capstone Requirement
- IS2000 Introduction to Information Science for MSIS, or one Human/Mgmt area requirement for MST

The SAIS capstone requirement is tailored towards facilitating students to develop skills in a particular practical IA issue. The CIO/AMP certificate course requirements significantly focus on the IA issues related to the federal systems and infrastructure and hence will be considered as having fulfilled a capstone requirement. IS2000 covers broad, current issues related to information sciences, which are addressed in the CIO/AMP courses.

Note that once the IRMC certificate holders complete the remaining requirements after transferring to DIST, they are eligible for all the five CNSS standards (CNSS 4011 to 4015). The SAIS curriculum requirements are more rigorous than the general MSIS degree requirements (although admissions requirements are essentially the same) and the SAIS students may have to take more courses than shown above.

Annex C – Overview of the Committee of National Systems Security (CNSS) standards

Pitt's SAIS curriculum has been certified for the CNSS standards 4011, 4012, 4013, 4014A and 4015. NDU/IRMC's IA curriculum has been certified for CNSS 4011 and 4012.

CNSS 4011 - NATIONAL TRAINING STANDARD FOR INFORMATION SYSTEMS SECURITY (INFOSEC) PROFESSIONALS:

This instruction provides the minimum course content for the training of information systems security (INFOSEC) professionals in the disciplines of telecommunications security and automated information systems (AIS) security.

CNSS 4012- NATIONAL TRAINING STANDARD FOR DESIGNATED APPROVING AUTHORITY (DAA)

This instruction establishes the minimum course content or standard for the development and implementation of training for Designated Approving Authorities in the disciplines of telecommunications security and information systems (IS) security.

CNSS 4013 - NATIONAL TRAINING STANDARD FOR SYSTEM ADMINISTRATORS IN INFORMATION SYSTEMS SECURITY (INFOSEC)

This instruction establishes the minimum course content or standard for the development and implementation of training for system administrator professionals in the disciplines of telecommunications security and information systems (IS) security.

CNSS 4014 - NATIONAL TRAINING STANDARD FOR INFORMATION SYSTEMS SECURITY OFFICERS (Advanced level)

This instruction establishes the minimum course content or standard for the development and implementation of training for Information Systems Security Officers (ISSO) in the disciplines of telecommunications security and information systems (IS) security. Please check with your agency for applicable implementing documents.

CNSS 4015 - NATIONAL TRAINING STANDARD FOR SYSTEM CERTIFIERS

This instruction establishes the minimum course content or standard for the development and implementation of education and training for System Certifier professionals in the disciplines of telecommunications security and information systems (IS) security. Please check with your agency for applicable implementing documents.

For more information on the CNSS standards, see:
http://www.nsa.gov/ia/academia/cnsstesstandards.cfm