Course Listing

AII

Information Assurance and Critical Infrastructure Protection (6203)

This course provides a comprehensive overview of Information Assurance and Critical Infrastructure Protection. Information assurance of information assets and protection of the information component of critical national infrastructures essential to national security are explored. The focus is at the public policy and strategic management level, providing a foundation for analyzing the information security component of information systems and critical infrastructures. Laws, national strategies and public policies, and strengths and weaknesses of various approaches are examined for assuring the confidentiality, integrity, and availability of critical information assets.

ARC

Enterprise Architecture for Leaders (6412)

This course examines enterprise architecture (EA) as a strategic capability organizational leaders use for enterprise planning, resource investment, management decision-making, and key process execution. Students explore leadership competencies and strategies needed to advance EA adoption and assess the integration of EA with governance, strategic planning, budgeting, portfolio management, capital planning, and information assurance. They critique EA prescriptive frameworks that guide EA development activities and review EA evaluative frameworks used to assess organizational EA management capacity and capability. Students evaluate challenges to organizational EA adoption and consider strategies to address them.

ATO

Approval to Operate: Information System Certification and Accreditation (6209)

This course examines the information security certification and accreditation principles leading to final Approval to Operate (ATO) an information system. The course examines roles, responsibilities, documentation, organizational structure, directives, and reporting requirements to support the Designated Accrediting Authority (DAA) in approving the security control functionality level of an information system and granting ATO at a specified level of trust. The course provides an overview of DOD and Federal department and agency certification and accreditation processes (e.g., Defense Information Assurance Certification and Accreditation Process; NIST Certification and Accreditation Process), information assurance acquisition management, and system security architecture considerations.

BCP

White House, Congress, and the Budget
(6606)

CFO Program students only

This course presents a strategic understanding of Federal budgeting and appropriations, with particular attention to the role of the White House and the Congress. With this critical understanding, students develop leadership strategies to shape the fiscal environment to achieve agency strategic outcomes. The course focuses on topics such as the impact of current fiscal issues including the competition between discretionary and nondiscretionary spending and its likely impact upon agency activities, the dynamic interaction between agency, executive, and Congressional committees and staffs in developing a budget and gaining an appropriation.

CAP

Capstone (6700)

The CAP course is the culminating learning experience of the Government Information Leadership (GIL) Master of Science Degree Program. While enrolled in CAP, students complete a capstone synthesis project in his or her area of concentration. The NDU iCollege department responsible for each Master of Science concentration will define the specific nature and detailed requirements for the type of project suitable for the respective concentration, and decide how a particular project type is assigned to a specific student.

CBL

Cyberlaw (6204)

This course presents a comprehensive overview of ethical issues, legal resources and recourses, and public policy implications inherent in our evolving online society. Complex and dynamic state of the law as it applies to behavior in cyberspace is introduced, and the pitfalls and dangers of governing in an interconnected world are explored. Ethical, legal, and policy frameworks for information assurance personnel are covered. Various organizations and materials that can provide assistance to operate ethically and legally in cyberspace are examined. Topics include intellectual property protection; electronic contracting and payments; notice to and consent from e-message recipients regarding monitoring, nonrepudiation, and computer crime; and the impact of ethical, moral, legal and policy issues on privacy, fair information practices, equity, content control, and freedom of electronic speech using information systems.

CFF

Changing World of the CFO (6601)

CFO Program students only

This course focuses on the changing environment for the government Chief Financial Officer (CFO). Students explore the fundamental role of the collaborative and networked community as the critical ingredient of success. The course provides an overview of the essential elements of the current and future roles of government CFO's and their senior staffs. It surveys the various roles of the executive and strategic leader in the world of government financial management including budget officer, compliance officer, internal controls/risk manager, strategic planner, fiduciary reporter, and reporter of management and financial information. The course discusses the policies, challenges and opportunities associated with decision support to management, financial reporting, business process improvement, systems integration, financial systems, workforce development, performance management, budget, and portfolio management. Students discuss standards, accountability, privacy, and transparency issues.

CIC

Campaigning in Cyberspace (6258) (SJSS Students only)

The course is centered on the Joint Operational Planning Process (JOPP) to solve strategic and operational problems and to further national interests, policies, and strategic objectives. This course begins with a review the Joint Operational Planning Process (JOPP), and then follows with identifying and analyzing the integration of information and cyber operations in theater strategy and campaign planning. As part of the course of study, students explore the national security concept of "strategic fragility" as it applies to modern society's growing reliance on interconnected, complex, and potentially fragile critical infrastructures. The course covers the rise of fragile infrastructures, the role of the information infrastructure as a control mechanism, sources of vulnerability, examples of infrastructure attacks and their consequences, and potential means to mitigate risks and deter attacks by others on our strategic infrastructures. It concludes with an exercise for students to put into practice the concepts learned in the course.

CIO

CIO 2.0 Roles and Responsibilities (6303)

Students examine the essential analytic, relational, technological, and leadership competencies that government CIOs and their staffs need to respond to and shape the 21st Century environment. Students assess the high information and IT demands of customers; examine the potential and perils of ubiquitous technology and information saturation; and weigh the tradeoffs of resource constraints, legal and policy mandates, and security in an open environment. The dynamic and multidimensional roles and responsibilities of government CIOs and their staffs are scrutinized to assess opportunities and challenges for improving governance, resource management, and decision making. Students analyze critical internal (CTO, CFO, Commander, Agency Head, Operations Chiefs) and external (other governmental agencies, OMB, Congress, and the private sector) relationships that CIOs and their staffs need to foster in order to satisfy their mission-related, legal, organizational, and political mandates.

CIP

Critical Information Infrastructure Protection (6230)

This course examines the security of information in computer and communications networks within infrastructure sectors critical to national security. These include the sectors of banking, securities and commodities markets, industrial supply chain, electrical/ smart grid, energy production, transportation systems, communications, water supply, and health. Special attention is paid to the risk management of information in critical infrastructure environments through an analysis & synthesis of assets, threats, vulnerabilities, impacts, and countermeasures. Students learn the importance of interconnection reliability and methods for observing, measuring, and testing negative impacts. Critical consideration is paid to the key role of Supervisory Control And Data Acquisition (SCADA) systems in the flow of resources such as electricity, water, and fuel. Students learn how to develop an improved security posture for a segment of the nation’s critical information infrastructure.

COO

Continuity of Operations (6504)

This course focuses on developing and implementing effective continuity of operations (COOP) plans in public sector agencies. Using federal regulations and policies as a backdrop, the course examines the technological, human capital, legal, and business factors involved in creating and maintaining a COOP plan. Topics include determining business requirements, selecting alternate sites, employing technology to increase organizational resilience, developing exercises, and creating and implementing emergency plans. Through a series of exercises, students develop skills in creating, evaluating and implementing continuity of operations policies and plans.

COT

Communications on Target (6161) (SJSS Students only)

Crafting a strategy for communicating messaging associated with whole of government policy and decision questions requires a knowledge of strategic analyses, channeling choices, communication modalities, and sensitivity analyses. This course builds competencies in these areas through a structured interplay of theory and application. Content covered includes executive level communications, strategic decision elements, decision option analyses, content crafting for various modalities, and communications strategy development. Students will demonstrate their abilities through a variety of activities to include the annual Atlantic Council Cyber 9/12 competition.

CYI

Cyber Intelligence (6232)

This course examines the cyber leader's role in cyberspace intelligence. As decision makers, cyber leaders both enable and consume intelligence related to cyberspace: as enablers, they formulate and implement intelligence policy and strategy, acquire and deliver enterprise level information technology ("strategic IT") systems, and plan, program, budget for, and execute intelligence programs in cyberspace; as consumers, they plan and execute intelligence activities in cyberspace or make decisions based on threats emanating in or through cyberspace. This course includes perspectives and issues applicable to the U.S. Intelligence Community (IC) in general and elements unique to cyberspace. It is not intended to impart intelligence-specific skills and tradecraft to professional intelligence officers, and no prior experience in or knowledge of intelligence is required.

DAL

Data Analytics for Leaders (6420) (replaced ASA)

This course examines how organizations can improve mission execution by employing data analytics capabilities. Establishing and maturing these capabilities requires leadership as well as an ability to both conduct analytics and interpret analytic results. Students will apply qualitative and quantitative measures on data sets to better enable organizations to meet mission needs and organization priorities. The quality of data and the sources from which data are collected are explored. Compliance, security and the 'ethical' use of data will also be topics of discussion within the course.

DMG

Decision Making for Government Leaders (6323)

This course examines the environment, opportunities, and challenges of leadership decision making in government agency and interagency settings from individual, managerial, and multi-party perspectives. Decision contexts and the consequences for federal government leaders and organizations are viewed using the multiple perspectives of governance, policy, technology, culture, and economics. Students actively explore and reflect on how and why decisions are made by immersing themselves into complex issue scenarios and using leading-edge decision tools.

DMS

Data Management Strategies and Technologies: A Managerial Perspective (6414)

This course explores data management and its enabling technologies as key components for improving mission effectiveness through the development of open, enterprise wide, and state-of-the-art data architectures. It examines management issues such as the implementation of the data component of the Enterprise Architecture specified by OMB. The course considers key data management strategies, including the DOD Net-Centric Data Strategy, and the Federal Enterprise Architecture (FEA) Data Reference Model and their enabling information technologies including data warehousing, electronic archiving, data mining, neural networks, and other knowledge discovery methodologies. Students explore data management issues and implementation. The course provides sufficient insight into the underlying technologies to ensure that students can evaluate the capabilities and limitations of data management options and strategies.

DRR

Directed Readings and Research (6691/6692/6693)

Variable credit (1-3 credits) independent readings and research related to a topic of special interest to the student. Written assessment required.

EIT

Emerging Information Technologies (6442)

This course examines the core concepts of information technology and its rapidly expanding role in solving problems, influencing decision making and implementing organizational change. Students will be introduced to an array of emerging information technologies at various levels of maturity. Students analyze how emerging information technologies evolve. They evaluate the international, political, social, economic and cultural impacts of emerging information technologies using qualitative and quantitative evaluation methods. Students assess emerging information technologies using forecasting methodologies such as monitoring and expert opinion, examining future trends, and assessing international perspectives.

ESS

Enterprise Information Security and Risk Management (6206)

This course explores three themes, based on the Certified Information Security Manager® (CISM®), critical to enterprise information and cyber security management areas: information security risk management, information security/assurance governance, and information security/ assurance program management. Examining the concepts and trends in the practice of risk management, the course analyzes their applicability to the protection of information. Information security/assurance governance is illuminated by exploring oversight, legislation, and guidance that influence federal government information security/assurance. The course explores the challenges of implementing risk management and governance through enterprise security/ assurance program management. This includes enterprise information and cyber security strategies, policies, standards, controls, measures (security assessment/metrics), incident response, resource allocation, workforce issues, ethics, roles, and organizational structure.

FCT

Foundations of the Cyberspace Terrain (6157) (SJSS Students only)

This course examines the fundamental concepts of the information environment and cyberspace from the whole of government, academic, and industry perspectives. Students examine the history, evolution and current technology of the human-made digital world, manifested in the establishment of the globally accessible Internet. Students examine the concept of cyberspace as a variation of all things digital and the military context of the Cyber domain.

FFR

The Future of Federal Financial Information Sharing (6607)

CFO Program students only

This course focuses on the vital role Chief Financial Officers and financial managers have in providing federal financial information. To fully support decision making, this actionable financial information must be timely, accurate, transparent, accountable, and result in “clean” audit opinions. To evaluate the quality of Federal financial information sharing, the course explores the current stovepipes of financial statements, budgetary reporting, program/project cost reporting, and financial standards, as well as a holistic view of crosscutting information such as financial and non-financial dashboards. In addition, successful financial information sharing in the current dynamic environment can be facilitated by financial systems, data management techniques, and effective communication with internal and external users.

GEN

Global Enterprise Networking and Telecommunications (6205)

This course focuses on the effective management of network and telecommunication technologies in a government sector global enterprise. The course examines current and emerging network and telecommunications technologies, including their costs, benefits, and security implications, placing emphasis on enabling military and civilian network operations. Topics covered include JIE, the role of cybersecurity risk in networks and technology deployment, joint spectrum management, data visualization for network security, DevOps and cloud migration, mobile computing and network policy / governance to promote innovation.

ICC

International Context of Cyberspace (6154) (SJSS Students only)

This course provides an overview of the issues surrounding transnational cyberspace by examining various global governance frameworks, cyber policies, international investment and economic strategies, and the advancement of innovation through information and communication technologies (ICT). Students explore cyberspace policies and strategies in use by various countries and regions, as well as the social, political, economic and cultural factors that lead to diverse international perspectives on cyberspace.

IPC

International Perspective on Cyberspace (6228)

This course provides an overview of the issues surrounding transnational cyberspace policies, international investment strategies, and implementation of information and communication technologies (ICT) that affect the global economy and transforms the flow of information across cultural and geographic boundaries. Students examine the cyberspace policies that empower ICT innovation, various global governance frameworks, and organizations that shape and transform cyberspace. Students explore the cyberspace policies and strategies of various countries and regions as well as the cultural factor that leads to various international perspectives on cyberspace. Students also learn how to anticipate and respond to surprise and uncertainty in cyberspace.

IPL

Information Technology Program Leadership (6411)

This course examines the challenges of Federal program leadership in an Information Technology (IT) context. Students gain theoretical insight, supplemented by practical exercises, covering a variety of program/project leadership concepts and techniques. Particular areas of focus include customer service, stakeholder relations, decision-making methods, processes and pitfalls, interpersonal skills, organizational awareness and dynamics, and written and oral communication skills. The course explores the role of oversight in the management and leadership of Federal IT acquisition programs.

ITA

Strategic Information Technology Acquisition(6415)

This course examines the role senior leaders in both government and industry play in the successful acquisition of information technologies and services to achieve strategic organizational goals. Using the framework of the systems development life-cycle, it explores regulatory policies, acquisition strategies, requirements management, performance measurement, and deployment and sustainment activities that directly impact IT acquisition. Acquisition best practices such as performance-based contracting, risk management, use of service-level agreements, trade-off analyses, as well as the pros and cons for use of commercial off-the-shelf products are explored. Significant focus is placed on contracting issues including; the role of the contracting officer, building a solid request-for -proposal, how to prepare for and run a source selection and the role of oral presentations.

IWS

Information, Warfare, and Military Strategy (6151) (SJSS Students only)

Prerequisite: Secret Clearance is required

This course examines key considerations for the planning and conduct of information operations at the theater and strategic levels. The course emphasizes inter-agency and international considerations in the planning and conduct of Information Operations (IO). Students examine selected non-U.S. approaches to the strategies for and uses of the full spectrum of information operations by current and potential global competitors and adversaries. They examine strategic legal implications and considerations and the use/misuse of IO strategies against an adaptive adversary. The course concludes with a snapshot of current U.S. military IO strategies.

ITP

Information Technology Project Management (6416)

This course focuses on project and program management in an Information Technology (IT) context, including financial systems. Students explore industry-accepted project management processes, e.g., the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK) framework, and apply project management concepts. Major topics include planning and management of project communications, scope, time, cost, quality, risk, human resources, procurement, and project integration. Factors that make IT projects unique and difficult to manage are explored, along with tools and techniques for managing them. This course challenges students to gain hands-on project management experience by performing complex project management tasks leading to the development of a project management strategy/plan.

LAW

Law, Authorities, and Warfare (6160) (SJSS Students only)

The course presents a comprehensive overview of the legal aspects of the cyber domain and the information instrument of national power. There are two overarching goals for students: first, to instill a broad, strategic-level understanding of the role of law in national security, and second, to provide a practical guide to the application of legal authorities in planning and executing cyber and information operations. The course introduces the student to legal reasoning, the relationship of law to technology and policy, and the sources of the domestic and international law. After providing students with a comprehensive ethical and moral framework for evaluating legal ends, ways, and means, the course provides an introduction to the global internet—its technological basis, the fundamentals of internet governance, and the complexities of jurisdiction in cyberspace. The course also addresses the conduct of military operations in cyberspace, specifically the jus ad bellum and the jus in bello. The course concludes with a legal and ethical exercise which will test the students' understanding of, and appreciation for, the role of law in shaping strategy and enabling, and limiting, large-scale national security operations.

LDC

Leadership for the Information Age (6301)

This course examines Information Age leadership and organizations. It describes the successful Information Age leader and organization as constantly learning and adapting to an increasingly complex, changing, and information rich environment. Emphasis is placed on “out-of-the-box” thinking, individual and organizational innovation, and the processes and structures that enhance an organization’s ability to learn, adapt, and compete in the Information Age. The course explores the role of information and technology in the Information Age organization; the relationships among learning, change, and strategic planning; and the new abilities required for leading in the Information Age.

MAC

Multi-Agency Information-Enabled Collaboration (6512)

The course focuses on multi-agency collaboration in support of national and homeland security and national preparedness planning, decision-making and implementation. It examines current and proposed strategies, means and models for substantially improving the effectiveness of collaboration at the federal, state and local levels, and beyond to include multilateral situations with non-governmental, media, and international organizations and coalition partners. The course assists students to synthesize the underlying principles that define effective collaboration, and critical lessons learned from past challenges and current experiments. Legal, budgetary, structural, cultural and other impediments that inhibit inter-agency mission effectiveness are assessed, as are strategies for addressing them. The course explores evolving network structures, collaborative tool-sets including social media, cross-boundary information-sharing and work processes, emergent governance arrangements, and the behaviors and skills of collaborative leadership as a key component of government strategic leadership.

NSC

National Security and Cyber Power Strategy(6329) (Previously CYS)

This course prepares students for strategic-level military and government leadership through the study of national security and cyberspace policies and strategies and their execution through cyber power statecraft. With an understanding of the U.S. national security architecture as a starting point, students explore the design components of national security strategy, including the instruments and resources of national power and the processes for formulating and stress testing national and subordinate level strategies. The course then focuses on the features of cyberspace as an evolving domain of national and international security, examining cyber power geopolitics and international relations strategies and statecraft. The course concludes with Project Solarium II - an exercise where students design and critique cyber power strategies to achieve desired scenario-based security outcomes.

NSS

National Security Strategy (6159) (SJSS students only)

This course prepares students for strategic level military and government service through the study of national security and cyberspace policies and strategies and their execution through cyber power statecraft. With an understanding of the components of a general theory of strategy and of the U.S. national security architecture as a starting point, students explore the design components of national security strategy, including the instruments and resources of national power. The course then focuses on the features of cyberspace as it continues to evolve as a domain of international security, examining cyber power geopolitics and international relations strategies and statecraft. The course concludes with a strategy game where students design cyber power strategies to achieve desired scenario-based outcomes.

OCL

Organizational Culture for Strategic Leaders (6321)

This course explores the strategic and persistent effects of culture on mission performance. Students examine the ways in which leaders can employ this powerful influence to nurture organizational excellence or to stimulate changes in organizational behavior. They investigate organizational sciences for traditional and Information Age perspectives on organizational behavior, on frameworks for assessing organizational cultures, and on strategies to initiate and institutionalize strategic mission-oriented change. Cross boundary, inter-agency, cross-generational, and global influences, issues, and challenges are examined from a cultural perspective.

ODC

Organizational Dynamics and Culture for Strategic Leaders (6150) (SJSS students only)

This course explores the strategic and persistent effects of internal and external dynamics on the health and performance of organizations. Students examine the ways in which leaders can assess, access, and influence organizational dimensions to promote organizational excellence and to stimulate positive changes in organizations. They examine theories and frameworks relevant to those dimensions to better understand organizational behavior and then apply strategies to initiate and institutionalize mission-focused change.

PFM

Capital Planning and Portfolio Management (6315)

This course focuses on state-of-the-art strategies for portfolio management, with an emphasis on assessing, planning, and managing information technology (IT) as a portfolio of projects from the perspectives of CIOs and CFOs. The three phases of the investment management process are considered: selection, control, and evaluation of proposals; on-going projects; and existing systems. The relationship of performance measures to mission performance measures is explored. The course examines the roles of the CIO, the CFO, and other managers in developing investment assessment criteria, considers how the criteria are used in planning and managing the portfolio, and explores the Office of Management and Budget's (OMB) portfolio perspective simulation of an IT investment portfolio review by the Investment Review Board.

PRI

Strategies for Process Improvement (6333)

This course examines strategies, management processes and resources for process improvement within and across Federal agencies. The course provides an executive-level examination of business process improvement strategies, including business process re-engineering, activity based costing/management, process architecting, Lean Six Sigma, and other quality improvement programs. An overview of the techniques and technologies that enable process-centric performance improvements in how agencies achieve their missions is provided. Attention is focused on the enterprise-level leadership challenges of process management, including initiation, collaboration, design, implementation, and portfolio project management of process-centric improvements within and across agencies.

RIA

Risk Management, Internal Controls, and Auditing for Leaders (6608)

CFO Program students only

This course presents a strategic understanding of risk management, internal controls, and auditing as they relate to the functions and responsibilities within the CFO and audit communities. This course examines how effective leadership can enhance efficiency, effectiveness, accountability, and transparency of an organization to include federal, state, and local governments. The primary focus is on the importance of identifying and assessing risks, describing and improving internal controls techniques and practices, and evaluating and recommending audit management strategies. The course includes practical discussions to illustrate how these processes can be integrated and leveraged to solve problems, make informed decisions, and minimize compliance costs.

RWS

Research and Writing Seminar (6093) (SJSS students only)

The Research Writing Seminar (RWS) provides students with an introduction to graduate-level research and writing. The course is designed to assist students as they work toward successful completion of the Individual Student Research Project (ISRP). This course examines research techniques, conducting a review of the literature, crafting cogent arguments, and the proper use and citation of sources. The goal is an ISRP that consists of at least 25-45 page of original work suitable for publication in a refereed journal. Students are evaluated on their quality of research, the innovativeness of their ideas, and the quality of the final paper. Students are also evaluated on their ability to present their findings to a committee composed of faculty and experts in the field.

SAC

Strategies for Assuring Cyber Supply Chain Security (6444)

This course explores the strategies necessary to manage global supply chain risk within the Department of Defense and across the federal government. Students examine how cyber leaders (i.e. CIO, CTO, and IT Program Managers) can secure the supply chain through an understanding of trusted mission systems, supply chain risks and the role of supply chain participants. Students address the challenge of assessing global supply chain risk and delivering reliable and secure technology to agency staff and the warfighter. They examine a range of disciplines including governance, intelligence analysis, legal and regulatory compliance, and software and information assurance.

SEC

Cyber Security for Information Leaders (6201)

This course explores concepts and practices of defending the modern net-centric computer and communications environment. The course covers the 10 domains of the Certified Information System Security Professional (CISSP®) Common Body of Knowledge (CBK®). It covers a wide range of technical issues and current topics including basics of network security; threats, vulnerabilities, and risks; network vulnerability assessment; firewalls and intrusion detection; transmission security and TEMPEST; operating system security; web security; encryption and key management; physical and personnel security; incident handling and forensics; authentication, access control, and biometrics; wireless security; virtual/3D Worlds; and emerging network security technologies such as radio frequency identification (RFID) and supervisory control and data acquisition (SCADA) security. The course also defines the role of all personnel in promoting security awareness.

SLFC

Phase 1: Strategic Leader Foundations Course (NDU 6000) (SJSS students only)

The SLFC will provide students with a common intellectual foundation essential for success at NDU and the CIC, and longer-term success as strategic leaders. The course will provide a foundation for developing the skills for creative and critical thinking; principles, skills, and challenges of strategic leadership; and an introduction to the strategic aspects of Joint Professional Military Education.

SLP

Strategic Leader Theory and Practice (6318) (CIO-LDP only)

This course focuses on the competencies of strategic leaders in theory and in practice across contemporary defense, government, and private sector organizations. Students evaluate, reflect upon, and refine their understanding of strategic leader strategies for leading and building effective organizations. They examine diverse organizations to draw insights they can apply to their organizations and their own practice of leadership. Key components of the course include individual awareness, team problem solving, oral and written communication skills, and studies with and about exemplar organizational leaders.

SPB

Strategic Performance and Budget Management (6328)

This course is an executive level view of strategic planning, performance management, and performance budgeting in public sector organizations. Using the Government Performance and Results Act and Kaplan & Norton’s Balanced Scorecard as frameworks, students examine the linkage of mission to strategic planning, performance management, measurement, operational strategies, initiatives, and budgets to support senior level decision making. Emphasis is on transparency, outcomes, and linkage between organizational performance and the organization’s budget. With this critical understanding, students develop leadership strategies that shape fiscal budgets to achieve agency strategic outcomes.

TCC

Terrorism and Crime in Cyberspace (6215)

This course explores the nature of conflict in the cyber realm by focusing on two major Internet-based threats to U.S. national security: cyber terrorism and cyber-crime. The course examines who is undertaking these cyber activities, what techniques they use, and what countermeasures can be adopted to mitigate their impact. The course provides a risk management framework to help information leaders leverage the benefits of Internet technologies while minimizing the risks that such technologies pose to their organizations.

WGV

Web-Enabled Government: Facilitating Collaboration and Transparency (6435)

This course explores the capabilities, selection, and application of new and emerging web technologies to enable more creative, collaborative, and transparent government. The course examines and assesses the use of current and emerging web technologies and best practices of significant government interest, e.g., cloud computing, social media and networking, geographic information services technology, and security. Students consider web technology evaluation criteria, methodologies, and risks to enable them to adapt the evaluation criteria and apply selected web technologies within and/or across government.

WSL

Warfighting at the Speed of Light (6162) (SJSS students only)

This course introduces students to concepts for emerging technologies and then challenges the student to explore their impact on current and future joint warfighting. Topics such as autonomous artificial intelligence systems, big data analytics on decision-making, interconnected ubiquity, and other technologies will be examined for their future impact on national security and joint warfighting. Students will also analyze the risks and ethical concerns associated with developing, integrating, and employing these technologies in the future operating