HLS 6000. Introduction to Homeland Security. 3 Hours.
Offers an overview of the essential ideas that constitute the emerging discipline of homeland security. Seeks to expand the way participants think, analyze, and communicate about homeland security and to assess knowledge in critical homeland security knowledge domains, including strategy, history, terrorism, fear management, crisis communication, conventional and unconventional threats, network leadership, weapons of mass destruction, lessons learned from other nations, civil liberties and security, intelligence and information, homeland security technology, and analytics. The course is organized around an evolving narrative about what homeland security leaders need and how the Center for Homeland Defense and Security program helps address those needs.

HLS 6010. The Unconventional Threat to Homeland Security. 3 Hours.
Introduces the operational and organizational dynamics of terrorism. Considers those who act as individuals, in small groups, or in large organizations and indigenous actors, as well as those who come to the United States to raise money, recruit, or commit acts of violence. In every instance, the focus is on violent clandestine activity that, whatever its motivation, has a political purpose or effect. Addresses such specific topics as suicide terrorism, the role of the media, innovation and technology acquisition, the decline of terrorism, and ways of measuring the effect of counterterrorism policies and strategies. The course also looks briefly at sabotage.

HLS 6020. Technology for Homeland Security. 3 Hours.
Offers individuals involved in homeland security a broad overview of homeland security technology, information systems, inspection and surveillance technology, communication, knowledge management, and information security. Government agencies in today’s information age are more dependent than ever on technology and information sharing. Focuses on technology as a tool to support homeland security personnel regardless of functional specialty. The methodology used in the course frames technology in terms of its contribution to deterrence, preemption, prevention, protection, and response after an attack.

HLS 6030. Intelligence for Homeland Security. 3 Hours.
Examines key questions and issues facing the U.S. intelligence community and its role in homeland security. The September 11, 2001, terrorist attacks on the World Trade Center and Pentagon and the ensuing war on terror have focused the nation’s attention on homeland security. Addresses policy, organizational, and substantive issues regarding homeland intelligence support. Course reference materials provide an overview of diverse intelligence disciplines and how the intelligence community operates. Emphasizes issues affecting policy, oversight, and intelligence support to homeland security and national decision making. Covers the 2004 Intelligence Reform and Prevention of Terrorism Act and focuses on homeland intelligence support issues at the state/local/tribal levels.

HLS 6035. Advanced Intelligence Applications for Homeland Security. 4 Hours.
Builds upon the analytical techniques discussed in HLS 6030 and develops actionable intelligence products. Offers students an opportunity to obtain an understanding of how intelligence is gathered and operationalized to support standing requirements and to support specific operations. One of the key roles of intelligence, especially in periods of active war and counterterrorism operations, is the nature, strengths, and weaknesses of intelligence intended to support operations in the field. This course describes how operational requirements are derived, transmitted to, and responded to by intelligence elements and how operational intelligence is collected, analyzed, and then used via practical, real-world situations. Open to U.S. citizens who hold a clearance of secret or higher.

HLS 6040. Critical Infrastructure: Vulnerability Analysis and Protection. 3 Hours.
Focuses largely on protecting the most fundamental critical infrastructures, one of the cornerstones of homeland security. Develops a network theory of vulnerability analysis and risk assessment called “model-based vulnerability analysis,” which is used to extract the critical nodes from each sector, model the nodes’ vulnerabilities by representing them in the form of a fault tree, and then applying fault and financial risk-reduction techniques to derive the optimal strategy for protection of each sector. At the completion of the course, students should be able to apply the model-based vulnerability technique to any critical infrastructure within their multijurisdictional region, derive optimal strategies, and draft policies for prevention of future terrorist attacks.

HLS 6050. Multidisciplinary Approaches to Homeland Security. 3 Hours.
Explores the homeland security project in relation to the laws that both support and constrain it. Homeland security efforts in the United States constitute a project framed by the rule of law. Constitutional concerns, civil rights issues, and the roles of the various disciplines engaged in the effort are driven and impacted by the various local, state, and federal systems of law. Uses both historical and contemporary references to unpack the various issues and answer related questions. While military, law enforcement, and judicial issues are a central concern of the course, considers the range of issues in relation to many other disciplines engaged in homeland security and defense.

HLS 6060. Strategic Planning and Budgeting. 3 Hours.
Examines a resource management system that allows decision makers to see the long-term implications of the decisions they are making today. Homeland security requires programs in such disparate areas as counterterrorism, information security, border security, counterdrug activities, etc. It also requires coordination of programs at the federal, state, and local levels. Covers how decision makers at the various levels decide which of these programs should be funded, the size approved programs should be and how they fit together, and how plans are translated into budgets. Studies an analytic approach to allocating resources in order to provide maximum security with limited budgets.
HLS 6070. Emergency Management and Geographic Information Systems. 3 Hours.
Explores how emergency management activities can best utilize geographic information technologies (GIT) to solve real-world issues in emergency management. This includes planning and response for both natural disasters and man-made events (accidental and terror-related incidents). Through the use of a variety of tools and analytical techniques, demonstrates and explores the nexus between emergency management and GIT. Exposes students to an understanding and appreciation for that relationship as well as the tools and skills for appropriate utilization of them.

HLS 6080. Continuity of Operations and Planning. 3 Hours.
Seeks to enable students to develop and implement continuity of operations (COOP) plans. COOP is a federal initiative, required by presidential directive, to ensure that executive branch departments and agencies are able to continue to perform their essential function under a broad range of circumstances. Today’s changing threat environment and recent emergencies have increased the need for COOP capabilities and plans. Topics include what COOP is and why it is important; how COOP differs from continuity of government (COG); the roles and responsibilities of key players in COOP planning; and family support measures to take in case of COOP implementation.

HLS 6090. Organization and Structural Continuity Planning. 3 Hours.
Covers the importance of protecting critical infrastructure and key resources (CIKR) for continuity planning. Identifies the relevant authorities and roles for CIKR protection efforts and describes the National Infrastructure Protection Plan unifying structure for the integration of CIKR protection efforts, including the sector security partnership model, the risk-management framework, and the information-sharing process. Offers students an opportunity to summarize critical infrastructure responsibilities; identify the range of critical infrastructure protection government and private-sector partners at the state, local, tribal, territorial, regional, and federal levels; describe processes for effective information sharing with critical infrastructure partners; and identify various methods for assessing and validating information as well as planning for continuity in the event of an emergency.

HLS 6100. Maritime and Port Security 1. 4 Hours.
Focuses on the elements of U.S. maritime and port security. With over 95 percent of the trade essential to U.S. economic well-being passing through hundreds of U.S. ports, the protection of port and waterways security is critical to homeland security. Examines U.S. and international policies, laws, and agreements governing maritime security, such as the Maritime Transportation Security Act and the International Ship and Port Security Code. Investigates the organizations responsible for maritime and port security in the United States as well as the potential U.S. and global impact of maritime security failures. Offers students an opportunity to explore the response and planning mechanisms for port security as well as irregular and transnational maritime security issues and their relation to the U.S. maritime transportation system.

HLS 6110. Maritime and Port Security 2. 4 Hours.
Develops the concepts covered in HLS 6100. Describes the International Port Security Program, which seeks to reduce risk to U.S. maritime interests, including U.S. ports and ships, and facilitates secure maritime trade globally. Discusses port security best practices and the development of mutual interests in securing ships coming to the United States, both U.S. port security and the security of the global maritime transport system. Discusses a port state’s implementation of the International Ship and Port Facility Code (ISPS Code) and other international maritime security standards to enhance port security measures beyond the minimum requirements of the code. Additionally, addresses the needs of foreign ports to provide mutual benefits to the United States and our maritime trading partners.

HLS 6120. Aviation Security 1. 4 Hours.
Analyzes the procedures, programs, systems, and security equipment that is currently used in the aviation industry. Reviews relevant legislation pertaining to aviation security from a historical and modern perspective. Also covers the history of terrorism in the aviation sector internationally and how these events have had an effect on aviation security to date and on the future of aviation security. Includes an overview of the many professional associations that play a large role in aviation security from an industry perspective and how they interact with the federal agencies that provide oversight of the aviation security industry. Emphasizes the structure and roles of the federal agencies involved in aviation security, physical security, and aviation legislation.

HLS 6130. Aviation Security 2. 4 Hours.
Continues HLS 6120. Introduces background and specific knowledge of the Transportation Security Agency (TSA), United States regulations, and the International Civil Aviation Organization (ICAO). The course is aimed at training airport executives and supervisory airport managers involved with establishing the direction, mutual aid agreement, and general security of the airport facility and operations. Focuses on planning, developing, and evaluating procedures and methods to secure the airport. Reviews specific content of the 49 Code of Federal Regulations 1542 (Airport Security) and ICAO Annex 17 (Safeguarding International Civil Aviation). Topics include airport security activities and awareness training, case study of practical crisis management exercises, and methodology and processes of law enforcement personnel in airport security.

HLS 6140. Port Security Capstone. 4 Hours.
Offers students an opportunity to utilize all of the port security (maritime and aviation) skills they have acquired to evaluate port and aviation security processes and outcomes of a single event throughout the entire event life cycle. Examines both quantitative and qualitative methodologies, with an emphasis on tactical approaches and strategic/long-range planning. Also examines stakeholder analysis and practical techniques for reporting performance results.

HLS 6192. Elective. 1-4 Hours.
Offers elective credit for courses taken at other academic institutions. May be repeated without limit.

HLS 6193. Topics in Homeland Security. 1-4 Hours.
Introduces selected and substantive issues in homeland security. Topics vary from one offering of the course to the next. May be repeated up to seven times for up to 8 total credits.

HLS 7000. Domestic Emergency Practicum in Homeland Security 1. 3 Hours.
Explores the history, features, principles, and organizational structure of the Incident Command System (ICS) and the relationship between ICS and the National Incident Management System (NIMS). Recognizes organizational culture, emphasizing the politically charged atmosphere in which it operates. Offers students an opportunity to obtain a clear understanding of how to operate efficiently during an incident or event within the ICS and the integration of the roles for primary departments and/or agencies during a local, state, and federal response, as well as the knowledge of how to apply critical resources for personnel who are likely to assume a supervisory position within the ICS.
HLS 7010. Domestic Emergency Practicum in Homeland Security 2. 3 Hours.
Introduces the National Incident Management System (NIMS), which provides a consistent nationwide template to enable all government, private-sector, and nongovernmental organizations to work together during domestic incidents. Also introduces the Multiagency Coordination Systems (MACS) as described within NIMS, which consists of a combination of the following elements: personnel, procedures, protocols, business practices, and communications integrated into one common system. Guides students through the National Response Framework, focusing on the principles that enable all response partners to prepare for and provide a unified national response to disasters/emergencies. Offers students an opportunity to learn how to improve the overall coordination with, and support for, incident management by developing and operating within MAC Systems.

HLS 7020. Domestic Emergency Practicum in Homeland Security 3. 3 Hours.
Explores unified command, incident/event assessment and objective development, the Incident Command System (ICS) planning process, incident/event resource management, transfer of command, and demobilization. Focuses on how major incidents create special management challenges, the circumstances in which an Area Command is established, and circumstances in which multiagency coordination systems are established. Examines the key players, their roles and responsibilities within ICS, processes for requesting and obtaining federal assistance, and understanding the emergency support functions that group federal resources and capabilities into functional areas to serve as the primary mechanisms for providing assistance essential in supporting all critical incidents.

HLS 7030. Domestic Emergency Practicum in Homeland Security 4. 3 Hours.
Seeks to familiarize students with Department of Defense (DOD) and other agency personnel in Defense Support of Civilian Authorities (DSCA) for domestic operations. Introduces national, state, local, and DOD statutes, directives, plans, command and control relationships, and capabilities with regard to DOD support for domestic emergencies, for designated law enforcement, and for disaster and emergency response. Focuses on interagency response to enhance the command leadership through specific decision-making processes. Finally, seeks to familiarize students with the plans and systems guiding the nation’s emergency response activities to provide a clear understanding of DSCA operations.

HLS 7040. Domestic Emergency Practicum in Homeland Security 5. 3 Hours.
Offers students an opportunity to develop leadership skills and organizational capabilities to respond to twenty-first-century homeland security emergencies. Uses intensive case-study-based discussion of recent events to develop concepts and frameworks for the design and execution of response in complex, multijurisdictional and multisectoral environments. Focuses on leadership and explores what leaders need to do before an event, how they need to operate during an event, and how they make the greatest possible contribution to the nation’s security. The course seeks to improve society’s capacity to deal with natural disasters; infrastructure, technology, and systems failures; infectious disease; terrorism; and to prepare emergency managers for success before, during, and after a catastrophic event.