Integrated Security

Background: Individuals and communities prosper in the presence of security, but required elements of security evolve and expand rapidly. Social, political, and financial networks connect individuals to communities, and communities to the world; infrastructure and commerce networks connect us to essential resources, and information networks store unprecedented amounts of data. These networks and assets allow us to explore opportunities and ensure the availability of water, shelter, food and energy. However, reliance on interconnected networks makes individuals and communities vulnerable to complex threads that have the same dynamical and multi-scale properties as the networks themselves.

This Destination Area seeks to identify, understand, and mitigate vulnerabilities to increase individual, community, national, and global security. This mission cuts across four other Destination Areas, intersecting at key points of national interest where Virginia Tech has developed considerable strength over its history of service. It is incumbent on Virginia Tech to work in partnership with government and industry to mitigate security vulnerabilities and to address the critical workforce and technology needs of state and federal and defense sectors.

Current Virginia Tech Differentiators/Objectives:

- Build upon robust education and research programs in critical infrastructure sectors — including energy, transportation, water, telecommunications, military platforms, environmental, agricultural, and financial networks — to address challenges in security. Enable homeland defense, develop national security policies, and promote global and international security.
- Leverage unique interdisciplinary expertise that spans science, technology, policy, and governance to produce well-rounded graduates that understand security challenges, while also enabling interdisciplinary research that creates innovative solutions to security problems and the trans-disciplinary knowledge required increase security in a complex world.
- Enhance the university's investment in the other Destination Areas by coupling security experts with domain experts to promote "security by design" in emerging technologies and systems.
- Engage faculty and students across colleges, institutes, the Corps of Cadets, and Reserve Officer Training Corps programs in security research and instruction.
- Reflect the university's land-grant mission and service ethic by contributing to national and international security while promoting environmental conservation and economic development.

Experience and Assets: Virginia Tech has a tremendous advantage: an existing collaborative, interdisciplinary infrastructure already dedicated to education and research in security and resiliency. This Destination Area supports the university's "binary star" strategy by leveraging existing strengths in national security, public policy, and cybersecurity that extend from Blacksburg to the National Capital Region. With strong, historical partnerships with industry, government agencies, and civil society organizations, the university can build on an existing network of employers, research sponsors, and collaborators. The university embarks in this area with well-developed programs in key fields including energy cybersecurity, automotive cybersecurity, embedded system security, wireless security, information security, social and civil security, environmental security, cybersecurity education, business analytics, biosecurity, food defense, security policy, and environmental security.

This interdisciplinary research ecosystem comprises college-, center-, institute-, and laboratory-level collaborations, including numerous NSF Industry/University Cooperative Research Centers. The Hume Center for National Security and Technology leads research in cybersecurity and resilience of national and homeland security and has developed interdisciplinary education. The Institute for Critical Technology and Applied Science has incubated and enabled much of the technology ecosystem with investments in relevant centers focused on wireless, big data, space and satellites, autonomous systems, and military platforms. The Virginia Tech Transportation Institute offers expertise in automotive safety and cybersecurity and the Biocomplexity Institute offers expertise in resilience of complex networks.

Within the social sciences and liberal arts, the Metropolitan Institute promotes research into community resilience, while the Department of Political Science, Center for Public Administration and Policy, and programs in Government and International Affairs conduct research into security governance. Collaborations between the colleges of Veterinary Medicine and Science have developed robust capability in biological and agricultural security. Aggregating these strengths across the university provides the capability for high-impact research, technology development, and creative policy programs, while enhancing external partnerships. Existing interdisciplinary education programs include a minor in cybersecurity; minors and majors in national security; and graduate certificates in homeland security, information assurance, and security studies. Additionally, there are security-oriented tracks in a number master's degree programs, including Information Technology, Political Science, and Public Health, along with numerous engineering majors, such as Computer Science and Computer Engineering, as well as Interdisciplinary Graduate Education Programs in global change, sustainable nanotechnology, water, and disaster resilience. Resources will be leveraged to develop the embedded majors and minors envisioned by the Beyond Boundaries initiative.

The university also operates infrastructure to uniquely participate in security research. With Biosafety Level 3 facilities, research on biological agents can be undertaken. In addition, the university operates secure research facilities to execute classified programs sponsored by defense and intelligence agencies, and employs nearly 100 researchers and support personnel with active security clearances.

Examples of Targeted Hot Spots:

- **Critical Infrastructure Protection:** Virginia Tech has the opportunity to be a leader in critical infrastructure protection, particularly in food, water, energy (conventional, renewable, nuclear), finance, and transportation systems, with integrated expertise from embedded control systems through effective regulation of private infrastructure to address public needs.
- **Cybersecurity Technology, Governance, and Citizenship:** As smartphones, the Internet of Things, cyber-physical systems, cloud computing, and software-defined networking reshape the cyber landscape, education and research initiatives will focus on human factors in cybersecurity, protecting personal data/metadata, and regulatory and policy frameworks for digital privacy.
- **Defense Technology, Strategy, Policy:** As strategic defense and intelligence initiatives expand beyond the past 15 years of counterterrorism to include emerging national threats, mission scope now ncludes areas where Virginia Tech has unique expertise, including nonproliferation, biodefense, nuclear security, aerospace platform resilience, and cyber defense.
- **Biological and Social System Security:** Biological data science and personalized medicine offer health benefits but raise security and privacy issues. Generation/aggregation of important data must be coupled with trusted, secure data computation and storage.