Michael A. Haney, PhD, CISSP

Idaho Falls, ID 83401 • (208) 243-8952 • m.haney@sawtoothdigitalforensics.com
linkedin.com/in/michael-haney-phd-cissp • orcid.org/0000-0003-2359-2478 • sawtoothdigitalforensics.com

EDUCATION

Doctor of Philosophy, Computer Science *May 2015*
University of Tulsa, Tulsa, OK

- Dissertation: *A Method for Preserving Privacy in Network Monitoring*
- Advisor: Dr. John Hale · Honors: H.G. Osborn Fellowship

Master of Science, Computer Science *December 2013*
University of Tulsa, Tulsa, OK

- Honors: Research Assistantships

Bachelor of Science, Mathematics (Physics minor) *May 1998*
University of Kentucky, Lexington, KY

- Honors: Phi Beta Kappa; Sigma Pi Sigma; Honors Program

CERTIFICATIONS AND LICENSES

Credential	Issuer	Date
Certified Information Systems Security Professional (CISSP)	$(ISC)^2$	2002, current
GIAC Certified Intrusion Analyst (GCIA)	GIAC	2005, current
GIAC Security Essentials Certification (GSEC)	GIAC	2006, current
GIAC Certified Incident Handler (GCIH)	GIAC	2008, current
GIAC Certified Forensic Analyst (GCFA)	GIAC	2012, current
Cybersecurity First Responder (CFR-310)	CertNexus	2020
Qualified Security Assessor (QSA)	PCI SSC	2009–2014
NSTISSI-4011: Information Systems Security Professional	CNSS	2013
CNSSI-4012: Senior Systems Manager	CNSS	2013
CNSSI-4014A: Information Systems Security Officer (Advanced)	CNSS	2014
CNSSI-4016A: Risk Analyst (Advanced)	CNSS	2014

ACADEMIC EXPERIENCE

Clinical Professor *August 2025 – May 2026*
Energy Systems Technology & Education Center, Idaho State University

- Developed and delivered two foundational AI courses supporting the Specialized Technical Certificate in Applied AI Systems at ISU's College of Technology: *Fundamentals of Applied and Industrial AI* and *Secure and Trustworthy AI Systems* (risk management, policy, ethics, and AI lifecycle considerations).

- Served on the University President's AI Task Force, co-leading the working group on the impact of AI on faculty, staff, and students; contributed to institutional AI integration strategy.
- Designed curriculum aligned with NSA CAE accreditation standards to position ISU for future Center of Academic Excellence designation.
- Initiated planning for faculty and industry bootcamps and integration of AI concepts into Industrial Cybersecurity, Cyber-Physical Systems, IT, and Networking programs.

Associate Professor of Research *August 2024 – May 2025*
School of Cyber Studies, University of Tulsa

- Graduate research faculty advising Cyber Fellows PhD students on research in critical infrastructure and cybersecurity education.
- Served on the committee to develop the University of Tulsa's AI Minor (available Fall 2025) and contributed to "AI + X" degree planning; developed two new courses on AI systems.
- Served on the University of Tulsa AI Impact Task Force, providing strategic direction for program development and secure and trustworthy AI implementation campus-wide.
- Assisted with externally funded research from the Department of Energy (CESAR) and the U.S. Secret Service's National Computer Forensics Institute (NCFI) Lab.

Associate Professor, Computer Science *July 2021 – May 2024*
University of Idaho, Idaho Falls

- Appointed Program Manager for the Idaho Cybersecurity Education Initiative and Director of the Idaho Cyber Range (FY21–FY23), coordinating curriculum and education efforts across eight Idaho institutions of higher education.
- Led a statewide team of stakeholders to design and build the Idaho Cyber Range from inception.
- Maintained joint appointment to Idaho National Laboratory's Cybercore Integration Center; affiliated with the Center for Advanced Energy Studies (CAES), the Center for Secure and Dependable Systems (CSDS), and the UI Nuclear Engineering and Industrial Management Department.
- Helped design and establish the PhD in Cybersecurity (first offered Fall 2025), the MS in Cybersecurity (Fall 2021), and the BS in Cybersecurity (Fall 2020).

Assistant Professor, Computer Science *August 2015 – June 2021*
University of Idaho, Idaho Falls

- Taught computer science and technology management with a focus on cybersecurity and critical infrastructure protection.
- Joint appointment to Idaho National Laboratory (INL) in Resilient Control and Instrumentation Systems; researcher at CAES; affiliate of CSDS.
- Established the Graduate Certificate of Critical Infrastructure Resilience (adopted 2017).
- Research focus: information assurance, cyber-physical control systems, active defense, incident response, and digital forensics.

Graduate Research Assistant *2011 – 2015*
Institute for Information Security, University of Tulsa

- DARPA- and USAF-sponsored research in large-scale enterprise intrusion detection, incident discovery, and situational awareness.
- National Institute of Justice–sponsored research on security issues in telematics systems in fleet trucks and private vehicles.

Academic Administrative Appointments

- Director, Idaho Cyber Range (2021–2024)
- Program Manager, Idaho Cybersecurity Education Initiative (2020–2024)

NON-ACADEMIC EXPERIENCE

Senior Security Consultant *2011 – 2013*
True Digital Security, Tulsa, OK

- Designed and managed an advanced network security monitoring platform for managed services; consulted on cybersecurity for regional energy-sector companies and state agencies.

Senior Security Consultant *2008 – 2011*
FishNet Security, Boston, MA

- Risk management and regulatory compliance guidance to SMBs, enterprises, and federal agencies.

Manager (Consultant) *2002 – 2008*
Ernst & Young, LLP, Boston, MA

- Managed engagement teams for Fortune 500 clients in the financial services industry.

Additional practitioner instruction and roles: UK Royal Military Police, Portsmouth (2015); USSS National Computer Forensics Institute, Hoover, AL (2014); USN SPAWAR, San Diego (2013); ConocoPhillips, Tulsa (2013); ISACA Oklahoma Chapter (2011); SANS Mentor, SANS Institute (2010–2011); Senior Security Analyst, WilTel Communications/Level 3 (2001–2002); Security Administrator, FCI Web Hosting (2000–2001); Network Technician, EarthLink/MindSpring (1999–2000).

TEACHING

Areas of Specialization

- Secure and Trustworthy AI Systems; Applied and Industrial AI
- Cyber-human-physical security, including ICS/SCADA and Internet of Things
- Critical infrastructure protection, security, and resilience
- Digital forensics (malware analysis, network forensics, anti-forensics)
- Information assurance, policy, risk management, and compliance
- Applied cryptography and privacy-enhancing technologies
- Security data visualization; honeypots and cyber deception

Courses Developed and Taught

AI and Emerging Technology (Undergraduate)

1. *Fundamentals of Applied and Industrial AI* — Developed and delivered for ISU's Specialized Technical Certificate in Applied AI Systems; supported AI Minor development at University of Tulsa. First offered Fall 2025.
2. *Secure and Trustworthy AI Systems* — AI risk management, policy, regulatory issues, ethics, and deployment lifecycle. First offered Spring 2026. Supported both the ISU Applied AI Certificate and the University of Tulsa AI Minor.

Graduate-Level Courses

- Advanced Information Assurance; Computer and Network Forensics; Fundamentals of Critical Infrastructure Resilience; Information Operations and Cyber Warfare; Advanced Forensics and Malware Analysis; Applied Cryptography, Internet Surveillance, and Privacy; Enterprise Defense; Information Security Policy, Governance, and Compliance; Seminar: Contemporary Issues in Computer Science.

Directed / Independent Studies

- Advanced Networking and Security; Advanced Forensics: Memory Analysis; ICS/SCADA Security; Mobile Malware Forensics; IT Services Management; Cyber First Responder; Software Defined Networking for Operations Technology; Advanced Security and Penetration Testing; Authentication; Computer Security and Information Assurance; Foundations of Server Management; Privacy Enhancing Technologies; Malware Analysis; Cyber-Physical Systems Instrumentation and Control; SIEM; Quantum Cryptographic Key Exchange; Reverse Engineering Hardware; ICS Cybersecurity; Honeypots and Deceptive Systems.

Curriculum and Program Development

- Established the Specialized Technical Certificate in Applied AI Systems, ISU College of Technology (rollout Fall 2026); developed its two foundational courses.
- Served on the committee to establish the University of Tulsa AI Minor (Fall 2025) and future "AI + X" degrees.
- Built BS, MS, and PhD Cybersecurity programs at University of Idaho from inception (BS Fall 2020; MS Fall 2021; PhD Fall 2025).
- Established the Graduate Certificate of Critical Infrastructure Resilience (adopted 2017), a 15-credit-hour cross-disciplinary program.
- Designed curriculum aligned with NSA CAE accreditation standards at ISU.

Student Advising

Advised to completion as Major Professor: PhD, Computer Science (4); MS, Computer Science (14); MS, Technology Management (5); MS, Cybersecurity (5). **Total: 28.**

Graduate committee service (20+ roles): PhD, Cybersecurity, University of Idaho (1, current 2025); PhD, Cyber Studies, University of Tulsa (2, current 2025); PhD, Computer Science (10); MS, Computer Science (8); MS/ME, Nuclear Engineering (4).

SCHOLARSHIP

[1] Taegan Williams, Tiffany Fuhrmann, and Michael Haney. RADICL CTF: Low-cost CTF platform for industrial control systems education. *Journal of the Colloquium for Information Systems Security Education*, 10(1), March 2023.

[2] Tiffany Fuhrmann, Taegan Williams, and Michael Haney. Cyber-physical shooting gallery: Gamification to address the IT-OT gap in cybersecurity education. *Journal of the Colloquium for Information Systems Security Education*, 10(1):29–34, March 2023.

[3] Sam J. Root, Porter Throckmorton, Jonathan Tacke, Jacob Benjamin, Michael Haney, and R. A. Borrelli. Cyber hardening of nuclear power plants with real-time nuclear reactor operation, 1. preliminary operational testing. *Progress in Nuclear Energy*, 162:104742, 2023.

[4] Sam J. Root, Porter Throckmorton, Michael Haney, and R. A. Borrelli. Simulated boron shimming cyberattack on pressurized water reactor. *Transactions of the American Nuclear Society*, 127(1), 2022.

[5] Nawaf Almolhis, Michael Haney, Fahad Alqahtani, and Khalid Makdi. Discovering and understanding the security issues in IoT cloud. *International Journal of Computer Science and Security (IJCSS)*, 13(6), 2019.

[6] Michael McGregor and Michael Haney. Quantum key exchange simulator. *Journal of the Colloquium for Information Systems Security Education*, 6(1), September 2018.

[7] Ananth A. Jillepalli, Daniel Conte de Leon, Yacine Chakhchoukh, Mohammad Ashrafuzzaman, Brian K. Johnson, Frederick T. Sheldon, Jim Alves-Foss, Predrag T. Tosic, and Michael A. Haney. An architecture for HESTIA: High-level and extensible system for training and infrastructure risk assessment. *International Journal of Internet of Things and Cyber-Assurance (IJITCA)*, 1(2):173–193, June 2018.

[8] Ananth A. Jillepalli, Daniel Conte de Leon, Frederick T. Sheldon, and Michael A. Haney. Enterprise-level hardening of web browsers for Microsoft Windows. *International Journal of Computing and Digital Systems (IJCDS)*, 7(5):261–274, September 2018.

[9] David Oliver and Michael Haney. Curriculum development for teaching critical infrastructure protection. *Journal of the Colloquium for Information Systems Security Education*, 5(2), March 2018.

[10] Daniel Conte de Leon, Christopher A. Goes, Michael A. Haney, and Axel W. Krings. ADLES: Specifying, deploying, and sharing hands-on cyber-exercises. *Computers & Security*, 2018.

[11] Daniel Conte de Leon, Antonius Q. Stalick, Ananth A. Jillepalli, Michael A. Haney, and Frederick T. Sheldon. Blockchain: Properties and misconceptions. *Asia-Pacific Journal of Innovation and Entrepreneurship (APJIE)*, 2017.

[12] John Peterson, Michael Haney, and R. A. Borrelli. An overview of the methodologies for cyber security vulnerability assessments conducted in nuclear power plants. *Nuclear Engineering and Design*, 346:75–84, May 2019. Best Paper Award, ANS Innovations in Nuclear Technology R&D, 2019.

[13] Liang Kong, Michael Haney, Carolina Lindemuth, and David Greer. Cyber security training: ANN as an evaluator and informant. *Journal of the Colloquium for Information Systems Security Education*, 2(1):6–12, 2014.

[14] Michael Haney. Leveraging cyber-physical system honeypots to enhance threat intelligence. In Sujeet Shenoi and Jason Staggs, editors, *Critical Infrastructure Protection XIII*, International Journal of Critical Infrastructure Protection, pages 209–233. Springer, 2019.

[15] Trevor MacLean, R. A. Borrelli, and Michael A. Haney. Cyber security modeling of non-critical nuclear power plant digital instrumentation. In Sujeet Shenoi and Jason Staggs, editors, *Critical Infrastructure Protection XIII*, International Journal of Critical Infrastructure Protection, pages 87–100. Springer, 2019.

[16] Nawaf Almolhis, Abdullah Mujawib Alashjaee, and Michael Haney. Requirements for IoT forensic models: A review. In *Advances in Security, Networks, and Internet of Things*, pages 355–366. Springer, Cham, 2021.

[17] Abdullah Alashjaee, Nawaf Almolhis, and Michael Haney. Mobile malware forensics review: Issues and challenges. Springer Nature, 2020.

[18] Abdullah Mujawib Alashjaee, Nawaf Almolhis, and Michael Haney. Mobile malware forensic review: Issues and challenges. In *Advances in Security, Networks, and Internet of Things*, pages 367–375. Springer, Cham, 2021.

[19] Robert Hiromoto, Michael Haney, Aleksander Vakanski, and Bryar Shareef. Toward a secure IoT architecture. In Yuriy Kondratenko, editor, *Advanced Control Techniques in Complex Engineering Systems: Theory and Applications*. Springer, 2019.

[20] Peter J. Hawrylak, Chris Hartney, Michael Haney, Jonathan Hamm, and John Hale. Techniques to model and derive a cyber-attacker's intelligence. In Boris Igelnik and Jacek M. Zurada, editors, *Efficiency and Scalability Methods for Computational Intellect*. Information Science Reference, 2013.

[21] Tiffany Fuhrmann, Taegan Williams, and Michael Haney. Cyber-physical shooting gallery: Gamification to address the IT-OT gap in cybersecurity education. In *26th Colloquium for Information Systems Security Education (CISSE 2022)*, November 2022.

[22] Taegan Williams, Tiffany Fuhrmann, and Michael Haney. Low-cost CTF platform for industrial control systems education. In *26th Colloquium for Information Systems Security Education (CISSE 2022)*, November 2022.

[23] Tim Klett and Michael Haney. A framework for critical infrastructure prioritization and dependency analysis. In *15th Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, Arlington, VA, March 2021.

[24] Abdullah Alashjaee and Michael Haney. Forensic requirements specification for mobile device malware forensic models. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, January 2021.

[25] Jacob Benjamin and Michael Haney. Non-proliferation of cyber weapons. In *2020 International Conference on Computational Science and Computational Intelligence, Symposium on Cyber Warfare, Cyber Defense, and Cyber Security (CSCI-ISCW)*, Las Vegas, NV, December 2020.

[26] Abdullah Alashjaee and Michael Haney. A framework for mobile malware forensics. In *2020 International Conference on Computational Science and Computational Intelligence, Symposium on Mobile Computing, Wireless Networks and Security (CSCI-ISMC)*, Las Vegas, NV, December 2020.

[27] Nawaf Almolhis and Michael Haney. IoT forensics: Pitfalls for privacy and a model for providing safeguards. In *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, December 2019.

[28] Michael A. Haney. Advances in cyber-physical system honeypots to enhance threat intelligence. In *13th Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, Arlington, VA, March 2019.

[29] Trevor MacLean, R. A. Borrelli, and Michael A. Haney. Cyber security modeling of non-critical nuclear power plant digital instrumentation. In *13th Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, Arlington, VA, March 2019.

[30] Ibukun A. Oyewumi, Ananth A. Jillepalli, Philip Richardson, Mohammad Ashrafuzzaman, Brian K. Johnson, Yacine Chakhchoukh, Michael A. Haney, Frederick T. Sheldon, and Daniel Conte de Leon. ISAAC: The Idaho CPS smart grid cybersecurity testbed. In *IEEE Texas Power and Energy Conference (TPEC)*, College Station, TX, February 2019.

[31] Ibukun A. Oyewumi, Ananth A. Jillepalli, Philip Richardson, Mohammad Ashrafuzzaman, Brian K. Johnson, Yacine Chakhchoukh, Michael A. Haney, Frederick T. Sheldon, and Daniel Conte de Leon. Attack scenario-based validation of the Idaho ICS smart grid cybersecurity testbed (ISAAC). In *IEEE Texas Power and Energy Conference (TPEC)*, College Station, TX, February 2019.

[32] Ananth A. Jillepalli, Daniel Conte de Leon, Ibukun A. Oyewumi, Jim Alves-Foss, Brian K. Johnson, Clinton L. Jeffery, Yacine Chakhchoukh, Michael A. Haney, and Frederick T. Sheldon. Formalizing an automated, adversary-aware, risk assessment process for critical infrastructure. In *IEEE Texas Power and Energy Conference (TPEC)*, College Station, TX, February 2019.

[33] Ananth A. Jillepalli, Daniel Conte de Leon, Brian K. Johnson, Yacine Chakhchoukh, Ibukun A. Oyewumi, Mohammad Ashrafuzzaman, Frederick T. Sheldon, Jim Alves-Foss, and Michael A. Haney. METICS: A holistic cyber physical system model for IEEE 14-bus power flow system. In *13th IEEE International Conference on Malicious and Unwanted Software (MALCON)*, Nantucket, MA, October 2018.

[34] Ananth A. Jillepalli, Daniel Conte de Leon, Mohammad Ashrafuzzaman, Yacine Chakhchoukh, Brian K. Johnson, Frederick T. Sheldon, Jim Alves-Foss, Predrag T. Tosic, and Michael A. Haney. HESTIA: Adversarial modeling and risk assessment for CPCS. In *14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 226–231. IEEE, 2018.

[35] Michael McGregor and Michael A. Haney. Quantum key exchange simulator. In *22nd Colloquium for Information Systems Security Education (CISSE 2018)*, New Orleans, LA, June 2018.

[36] Michael McGregor, Zach Lontz, Daniel Conte de Leon, and Michael Haney. Network air locks, not air gaps, to preserve LAN security. In *23rd Colloquium for Information Systems Security Education (CISSE 2019)*, Las Vegas, NV, June 2019.

[37] Robert E. Hiromoto, Michael Haney, and Aleksander Vakanski. A secure architecture for IoT with supply chain risk management. In *9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*, Bucharest, Romania, September 2017. IEEE.

[38] Ananth A. Jillepalli, Daniel Conte de Leon, Stu Steiner, Frederick T. Sheldon, and Michael A. Haney. Hardening the client-side: A guide to enterprise-level hardening of web browsers. In *IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing (DASC/PiCom/DataCom/CyberSciTech)*, pages 687–692. IEEE, 2017.

[39] David Oliver and Michael Haney. Preparing the next cyber-resilient workforce through cross-pollination education. In *Resilience Week (RWS)*, Wilmington, DE, September 2017. IEEE.

[40] David Oliver and Michael Haney. Curriculum development for teaching critical infrastructure protection. In *21st Colloquium for Information Systems Security Education (CISSE 2017)*, Las Vegas, NV, June 2017.

[41] Ananth A. Jillepalli, Frederick T. Sheldon, Robert K. Abercrombie, Michael Haney, and Daniel Conte de Leon. Security management of cyber physical control systems using NIST SP800-82r2. In *13th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2017.

[42] Timothy McJunkin, Craig G. Rieger, Aunshul Rege, Saroj K. Biswas, Michael Haney, Michael John Santora, Brian K. Johnson, Ronald Laurids Boring, D. Subbaram Naidu, and John F. Gardner. Multidisciplinary game-based approach for generating student enthusiasm for addressing critical infrastructure challenges. In *ASEE Annual Conference & Exposition*, New Orleans, LA, June 2016.

[43] Matthew L. Hale, R. F. Gamble, John Hale, Michael Haney, Jessica Lin, and Charles Walter. Measuring the potential for victimization in malicious content. In *IEEE International Conference on Web Services (ICWS)*, pages 305–312. IEEE, 2015.

[44] Liang Kong, Michael Haney, and Carolina Lindemuth. Cyber security training: ANN as an evaluator and informant. In *18th Colloquium for Information Systems Security Education*, San Diego, CA, June 2014.

[45] Conor Fellin and Michael Haney. Preventing mistraining of anomaly-based IDSs through ensemble systems. In *IEEE Services 2014, 2nd Cloud Security Auditing Workshop*, June 2014.

[46] Michael Haney and Mauricio Papa. A framework for the design and deployment of a SCADA honeynet. In *Proceedings of the 9th Annual Cyber and Information Security Research Conference (CISR)*, pages 121–124. ACM, 2014. Best Paper Award.

[47] George Louthan, Michael Haney, Phoebe Hardwicke, Peter Hawrylak, and John Hale. Hybrid extensions for stateful attack graphs. In *Proceedings of the 9th Annual Cyber and Information Security Research Conference (CISR)*, pages 101–104. ACM, 2014.

[48] Peter J. Hawrylak, Michael Haney, Mauricio Papa, and John Hale. Using hybrid attack graphs to model cyber-physical attacks in the smart grid. In *5th International Symposium on Resilient Control Systems (ISRCS)*. IEEE, 2012.

[49] R. A. Borrelli, Jacob Benjamin, and Michael Haney. Cyberweapon nonproliferation controls for the virtual battlefield: Applying the nuclear nonproliferation regime to an unseen enemy. In *American Nuclear Society (ANS) Winter Meeting*, Washington, DC, December 2021.

[50] John Peterson, R. A. Borrelli, and Michael Haney. Advancement in methodologies for cyber security vulnerability assessments conducted in nuclear power plants. In *American Nuclear Society (ANS) Winter Meeting*, Washington, DC, November 2019.

[51] Tim Klett and Michael Haney. Critical infrastructure interdependencies. In *Military Operations Research Society (MORS) 87th Symposium*, Denver, CO, June 2019.

[52] Tim Klett, Ron Fisher, and Michael Haney. Effective metrics for determining critical infrastructure interdependencies. In *Industrial Control Systems Joint Working Group (ICSJWG) Spring Meeting*, March 2019.

[53] David A. Oliver and Michael Haney. CISR graduate certificate and foundations course development. Technical Report INL/CON-17-41444, Idaho National Laboratory, Idaho Falls, ID, 2017.

[54] John Peterson, Michael Haney, and R. A. Borrelli. Cybersecurity vulnerability assessment methodologies for nuclear power plants. In *2017 American Nuclear Society Annual Meeting*, San Francisco, CA, June 2017.

[55] Craig Rieger, Indrajit Ray, Quanyan Zhu, and Michael Haney, editors. *Industrial Control Systems Security and Resiliency: Practice and Theory*, volume 75 of *Advances in Information Security*. Springer Nature, 2019.

[56] Daniel Conte de Leon, Dilshani Sarathchandra, Kristin Haltinner, Kevin Chang, Francesco Mercaldo, Jia Song, Michael Haney, and Jim Alves-Foss, editors. *Proceedings of the 2016 Cybersecurity Symposium (CyberSec-2016)*. IEEE, Coeur d'Alene, ID, 2016.

[57] Michael Haney. System, method, and apparatus for computer security monitoring, information sharing, and collective intelligence. U.S. Patent No. 10,326,803 B1, June 2019. Provisional Application No. 62/031,023, filed July 30, 2014; issued June 18, 2019.

Externally funded research total: $18M+ (see Grants section). **Patents:** U.S. Patent No. 10,326,803 B1 (2019).

GRANTS AND CONTRACTS AWARDED

Project	Sponsor	Role	Amount	Period
Developing Industrial Cybersecurity Programs in East Idaho	NIST	Co-PI (McBride)	$2,875,000	2024–
HERC IGEM: Library of Reconfigurable Immersive Attack & Defend Scenarios	Idaho SBOE	PI	$2,097,000	2022–2025
CyberCorps Scholarship for Service (Renewal)	NSF	Co-PI	$1,410,908	2022
INL Haney Joint Appointment FY24	INL	PI	$94,505	2023–2024
Cybersecurity High School Innovation (CHI)	NSA	Co-PI	$34,270	2021–2025
INL Haney Joint Appointment FY23	INL	PI	$71,828	2022–2023
INL Haney Joint Appointment FY22	INL	PI	$70,397	2021–2022
INL Haney Joint Appointment FY20	INL	PI	$65,410	2019–2020
Multi-University SMR Simulators: NuScale	DOE/NEUP	Co-PI	$285,763	2019–2020
INL Haney Joint Appointment FY19	INL	PI	$72,853	2018–2019
CAES Summer Faculty Award	CAES	PI	$20,000	2018
CAES Seed Grant for Smart Grid Resiliency	CAES	Co-PI	$30,000	2018
INL Haney Joint Appointment FY18	INL	PI	$64,800	2017–2018
INL Haney Joint Appointment FY17	INL	PI	$63,500	2016–2017
IGEM: Security Management of Cyber Physical Control Systems	Idaho SBOE	Co-PI	$2,100,000	2016–2019
NSF SFS: Renewal of UI CyberCorps Scholarship for Service	NSF	Co-PI	$3,700,000	2016–2021
Resilient, Scalable Cyber State Awareness of ICS Networks	INL LDRD	Co-PI	$875,000	2016–2019
Dynamics of Multi-Layer Complex Infrastructure Networks	INL LDRD	Co-PI	$600,000	2016–2019

Project	Sponsor	Role	Amount	Period
Large Scale Log Analysis for Control System Networks	INL LDRD	Co-PI	$275,000	2016–2019
Modeling and Spatial-Temporal Analysis of Cyber-Physical Impacts	INL LDRD	Co-PI	$1,350,000	2016–2019
Hardware Request Grant: Titan X	nVidia	PI	$4,000	2016

Total externally funded research: $18M+

Amounts shown are award totals or Haney's share as listed; several INL joint-appointment renewals reflect a cumulative contract exceeding $642,000.

SERVICE

AI Governance and Task Force Leadership

- **ISU President's AI Task Force** — Co-led the working group on the impact of AI on faculty, staff, and students; contributed to institutional AI integration strategy (Aug–Dec 2025).
- **University of Tulsa AI Impact Task Force** — Provided strategic direction for program development and secure and trustworthy AI implementation campus-wide (Jan–May 2025).

Major Committee Assignments

- College of Technology Rank and Promotion Committee, ISU (2025)
- Hardware & Software Committee, CS Dept., UI (2020–2024)
- Curriculum & Petitions Committee, CS Dept., UI (2015–2020)
- IGEM Computer Science faculty search committees (2016–2018); CAES Director Search Committee (2017); Third-Year Review Committee for Dr. Daniel Conte de Leon (2015)

Advisory Boards and Technical Committees

- **Assistant Secretary, Board of Directors**, CISSE (Colloquium for Information Systems Security Education) — Elected to the national governing board (Jan 2026–present).
- Advisory Board Member, ISU ESTEC Energy Systems Cyber-Physical Security Program (2016–2025)
- Advisory Board Member / Technical Advisor, College of Eastern Idaho Cybersecurity and AgTech Programs (2017–2025)
- Advisory Board Member, BSides Idaho Falls Conference (2019)
- Technology/Cybersecurity Consultant, IRB, University of Tulsa (2013–2015)

Conference and Outreach Service

- **Co-Chair and Sponsorship Lead**, 30th Anniversary CISSE Colloquium, Indianapolis, IN (Jan 2026–present) — Direct a subcommittee-based sponsorship campaign ("$30K for the 30th") across a six-tier sponsor program; manage sponsor prospecting, tracking, and relationship management from outreach through signed commitment.
- **Lead, Competition & Games Subcommittee**, 30th Anniversary CISSE Colloquium (Jan 2026–present) — Designed new conference programming, including a cyber-domain competitive game and an infrastructure-security site tour, for the conference's milestone 30th-anniversary edition.
- Session Chair, IFIP WG 11.10 International Conference on Critical Infrastructure Protection (2021, 2019)
- Program Committee, 24th Colloquium for Information Systems Security Education (2020)
- Workshop Co-Chair, Cyber Resilient Supply Chain Technologies (CReSCT) Workshop, IEEE S&P (2020)

- Conference Technical Program Chair / Co-Chair, Cybersecurity Symposium (2018, 2017, 2016)
- Chair / Co-Chair, Cyber Track, Resilience Week (2018, 2017, 2016)

Professional Organizations

- $(ISC)^2$ Idaho Chapter Charter Member; IFIP WG 11.10; ACM; IEEE; ISSA (Senior Member); InfraGard; I3P

Selected Invited Talks and Presentations

- "AI Risks and Concerns" — Regional Economic Development Initiative, east Idaho business and government leaders (2025)
- "Secure and Trustworthy AI" — Guest lecture, Digital Literacy course (2025)
- "Cyberweapon Non-proliferation" — Keynote, 5th Annual BSidesOK (2019); also BSidesIF (2019)
- "Replacing Air Gaps with Air Locks for Better Network Security" — I3P Webinar Series (2019)
- "Cybersecurity and the Fourth Industrial Revolution" — Invited panelist, City Club of Boise (2019)
- "Privacy-Preserving Network Surveillance" — Boise State CS Colloquium (2020); Tulsa Cyber Summit (2019)

Community Service and STEM Outreach

- Xperiential Robotics Program (XRP) — AgXRP development team; DIY precision-agriculture build kits for east Idaho schools (2025–present).
- Cybercore Summer Camp / Advanced Cybercore Summer Camp — developed and delivered full curriculum; grew from local to statewide (2018–2023).
- STEM Senior Projects Mentor (six regional high school students); CISSP Bootcamps, UI CTOC, hosted in RADICL-IF (2017).

HONORS AND AWARDS

- **Best Article of the Year**, Energy Policy / Innovations in Nuclear Technology — American Nuclear Society, 2019 (Peterson, Borrelli, and Haney, *Nuclear Engineering and Design*, vol. 346).
- **Best Paper Award** — 9th Annual Cyber and Information Security Research Conference (CISR), ACM, 2014 (Haney and Papa, "A Framework for the Design and Deployment of a SCADA Honeynet").
- **"Brightest Star" Award** — Serve Idaho Program, Idaho Department of Labor, for service in high school STEM education and summer camps (January 2020).
- **CAES Employee of the Month** — "CAES Research, Education, and Innovation Leadership" (May 2019).

PROFESSIONAL DEVELOPMENT

- Workshop on Atomic Red Teaming — Wild West Hacker Fest (2020)
- Qualified as Instructor, Cyber First Responder Certification (2020)
- Workshop on Gamification of Cybersecurity Education — Las Vegas (2019)
- CAE Community Meeting — Las Vegas (2019); Huntsville (2017)
- Industrial Control Systems Cyber Security (301) Training — US DHS / ICS-CERT, Idaho Falls (2016)
- Cybersecurity for Nuclear Safeguards — IAEA and PNNL, Richland, WA (2016)
- NSF Grants Conference — Portland, OR (2016)

Curriculum vitae updated July 2026 · ORCID 0000-0003-2359-2478