NAVIGANT

Matthew M. Blizard

Matthew M. Blizard
Director

Navigant Consulting, Inc.
35 Iron Point Circle, Suite 225
Folsom, CA 95630
Tel: 916-631-3252
Fax: 916-852-1073

matt.blizard@navigant.com

Professional History

- Director, Navigant Consulting, Inc.
- Director, Critical Infrastructure Protection, North American Electric Reliability Corporation (NERC)
- Captain (retired), United States Coast Guard

Education

- M.S., National Security and Resourcing, National Defense University, Industrial College of the Armed Forces
- M.S., Computer Science, Rensselaer University (Hartford)
- M.S., Electrical Engineering, Purdue University
- B.S., Electrical Engineering, United States Coast Guard (USCG) Academy

Professional Associations

- Professional Engineer, Washington State
- American Society for Industrial Security (ASIS) Member

Honors and Fellowships

- Legion of Merit, USCG
- Meritorious Service Medal (Three)
- Commendation Medal (Five)
- Global War on Terrorism

Matthew Blizard is a Director in Navigant's Energy Practice. With three decades in security, law enforcement, and operations and mission support activities, Matt is well versed in providing clients with guidance on critical infrastructure protection (CIP) electric system reliability and security, national and homeland security, mission assurance, and program and performance management.

Prior to joining Navigant, Matt was the Director, CIP, at NERC. Matt led an experienced team of cyber and physical security professionals whose work focused on strengthening the reliability and security posture of the bulk power system (BPS). The CIP team did this by enhancing CIP standards (CIP v3, CIP v5, and CIP-014); supporting CIP transitioning efforts (Pilot Studies); building capability and capacity of the Electricity Sub-Sector Information Sharing and Analysis Center (ES-ISAC); conducting outreach (Security Reliability Program); supporting the recent cyber framework build and National Infrastructure Protection Plan revisions; and improving readiness through programs such as security exercises known as "Grid Ex", and the annual fall BPS security conference – "GridSecCon." Matt is the former secretary of the Electricity Sub-Sector Coordinating Council, and oversaw the Critical Infrastructure Protection Committee's (CIPC's) strong actions with task forces and work groups addressing reliability and security needs of the BPS. He focuses on enhancing strategic security, sustaining tactical actions to address evolving security threats, and closing vulnerabilities.

Before NERC, Matt served 30 years of commissioned service with the U.S. Coast Guard, leading, managing, and achieving multiple commands throughout his Coast Guard career. His assignments included the following: security; law enforcement; search and rescue operations; Command, Control, Communications, Computers and Information Technology (C4IT); mission support; and policy development. Matt's final Coast Guard assignment was as Deputy Chief of Staff and Executive Director to the Deputy Commandant for Mission Support, focusing on mission support transformation of engineering logistics, human resources, C4IT, acquisition efforts,

and the CG security program. His transformational activities concluded with testing of the service's new mission support structure, with earthquake relief efforts in Haiti and Deepwater Horizon oil cleanup.

Professional Experience

Electric System Reliability and Security

Matt directed the CIP of the bulk electric system (BES) (cyber and physical security) with NERC following his highly successful thirty-year career in the Coast Guard. At NERC, he formulated and executed a multitiered security strategy for the BPS, including mandatory standards, compliance actions, information sharing and analytics, private-public partnerships, and outreach, training, and exercises. More specifically, this strategy included the following:

» Oversaw and executed the BES security strategy, addressing never-ending cyber and physical threats with 1,800 plus entities across North America, coordinating with numerous federal agencies (U.S. Department of Energy [DOE], U.S. Department of Homeland Security [DHS], and U.S. Department of Defense [DOD]), reporting to a regulator, enhancing partnerships with Canadian officials, and leading teams of cyber and physical security experts.

» Designed CIP strategy to be fully actionable, nimble, and flexible to adjust to evolving threats and system vulnerabilities. BES multitiered security strategy included: enhancing mandatory and evolving cyber standards; overseeing compliance and enforcement of aggressive cyber standards; building an enhanced Information Sharing and Analytics (ISAC) center; maturing a highly regarded Alerts and Notifications System; partnering with government and industry cyber experts; designing a crisis action plan; pursuing an aggressive outreach, training and, exercise effort; and investigating High Impact Low Frequency events and hence associated actions to strengthen and secure the BES.

» Built a highly powerful cyber and physical security workforce at NERC, which included the following: recruited and hired CIP subject matter experts to understand and track security threats to the bulk power system; built CIP standards appropriately; conducted outreach; and developed security solutions through industry-led technical teams and work groups. The objective was to detect, defend, and protect the bulk power system's critical infrastructure to ensure reliability.

» Executed an $8M dollar security budget with multiple security contracts, including 17 cyber and physical security NERC specialists as the nucleus of the BES security operation.

» Recently integrated a White House and DOE-led Cybersecurity Risk Management Maturity Model (C2M2) into NERC's current Cyber Risk Preparedness Assessments ongoing in the BES. The model will determine programmatic shortfalls in security and will assist security managers and executives in determining what actions to take to improve security, and resourcing decisions.

» For NERC Board of Trustees, directed a 24-member technical Executive CIPC) overseeing 200+ cyber and physical security specialists in the pursuit of addressing pertinent and relevant cyber and physical security issues. Pursuits included: a High Impact Low Frequency Coordinated Action Plan; Cyber Attack Task Force; BES Security Metrics Work Group; BES Security Clearances Work Group; Cyber Security Information Sharing Task Force; Physical Security Working Group; Grid Exercise Working Group; Compliance and Enforcement Work Group; Control Systems Work Group; and Security Training Work Group.

» Revised and built a highly successful CIP outreach program at NERC, which included: designing and executing the largest bulk power system annual security conference (GridSecCon) where strategists, CEOs, and cyber and physical security experts from North America convene to discuss CIP threats and solutions;, and a robust Security Reliability Program (SRP) where NERC and Regional CIP experts work one on one with entities to understand evolving CIP standards, security threats, and how to ensure readiness for both cyber and physical compliance.

» Served as program sponsor for multiple CIP activities: CIP v5 standards development; CIP pilot studies to understand the challenges and issues faced by industry in the transition to CIP v5 so as improve the transition efficiencies and effectiveness; CIP-014 physical security standard development and its associated stand-up; multiple CIPC cyber technical reports on High Impact Low Frequency issues; updating of two physical security guidelines for industry; and Information Sharing, Cyber Attack, Resilience, and GridEx reports.

» Designed, advocated, and initiated a Physical Security Strategy and Readiness effort at NERC in 2014 to assist Registered Entities (volunteers) with their physical security pursuits to understand and implement CIP-014; to understand and capture the latest threat information regarding their facilities; to develop appropriate security plans and precautions; and to implement those security plans.

Executive and Organizational Leadership

» As the Coast Guard's Mission Support Executive Director and as the Chief of Staff's Deputy, oversaw enterprise-wide transformation efforts with adoption of industrial/DOD best practices. Transformed the Service's asset support system to include maintenance and logistic systems for the fifth largest maritime service in the world. This was the Service's largest transformational change since World War II. Developed a modernized support organization capable of delivering a unified logistics system based upon a bi-level maintenance model consisting of depot/unit-level maintenance and configuration management.

- Managed the daily inflow/outflow processes, services, and products of the Coast Guard. Required oversight with the Coast Guard's multimillion dollar ship/aircraft acquisition efforts; fleet sustainment programs; congressional/General Accounting Office coordination; mission support budget planning/execution efforts across departments; and daily coordination with DHS senior staffers, Coast Guard executive management (VP equivalents), down to all the department/division managers. Management and administration required significant technical skill and political astuteness, with a keen ability to "close the deal" with hugely diversified and geographically separated sets of individuals.

- Led—for the Coast Guard's Chief of Staff—the tactical support actions of the agency's engineers, logisticians, administrators, technicians, and human resource specialists, and astutely administered a $4.7B budget.

- Served as the Technical Administrator (Executive Director) for the combined Coast Guard aerospace, naval, shore facility, C4IT, logistics, human resource systems, and architectures for the entire 50,000 plus organization.

- Managed sustainment of Coast Guard's $19B fleet of ships, aircraft, and extensive shore infrastructure as Coast Guards Chief Engineer's Executive Administrator and technical authority.

- Oversaw human resource development, workforce health, diversity improvements, and developed policy and programs in accordance with DHS management requirements and budgetary expenditures.

- Shaped and executed national-level government policy in support of the White House and Office of National Drug Control Policy Interdiction Program. Assessed effectiveness of policy, plans, and the employment of assets; and insured the coordination of all aspects of international drug interdiction through department, agency, embassy, and military command staffs throughout the world. Served as specialist in the development of policy across agencies, preparation of congressional briefings, and the simulation and modeling of operational capabilities. Examined drug smuggling as a business and target interdictions to disrupt the business and dollar flows of the drug trafficking organizations (DTOs) (i.e., a strategic view of how to bankrupt the DTOs).

- Prepared principals on numerous occasions for Capitol Hill testimonies regarding drug/supply reduction policy efforts, legacy fleet sustainment efforts, and diversity actions ongoing within the Coast Guard.

Strategic Analysis, Engineering/Logistics, and Problem Solving

- Oversaw and directed Coast Guard logistic support–aircraft, ships, people, and supplies—for both Haitian earthquake efforts and Deepwater Horizon cleanup operations. (Legion of Merit awarded.)

» Provided insightful program, policy, and administrative guidance to senior executives with significant impact regarding engineering and logistics support and products produced, including the following: USCG Yard of the Future; Legacy Asset Sustainment; Configuration Management; Capital Asset Management; High-Performing Organizations; Product Line Development; Centralizing Boat Maintenance; and DHS efficiency efforts.

» Directed the largest counter-drug effort stemming the flow of illegal aliens and drugs. Planned, supported, and executed operations daily, working with 23 countries, three embassies, and an interagency task force made up of multiple federal and local agencies, spanning the Caribbean. Coordinated logistics, maintenance, and administrative daily support for 20+ cutters rotating every two months. Built a complex intelligence program, leveraging classified C4IT, human intelligence networks, and our international law enforcement partners.

» Led "train the trainer" operations in South/Central America; developed navies and emerging Coast Guards; built C2 capabilities, logistic, and maintenance systems; and established training programs.

» As a National Security and Homeland Security Strategist, applied critical thinking when examining different sides of an issue, looking for second and third order effects and ripple effects, taking a close look at security and resourcing ramifications. Modeled drug interdiction efforts to improve operational effectiveness, maximized valuable national resources, and developed a framework to justify additional resources with Congress. The system was called Interdiction Planning Asset Management Group (IPAMG).

Technical Authority/C4IT Program Management

» Pioneered Coast Guard's initial Cyber Command stand-up, laying framework and establishing mission set for new unit within DHS and the National Security Agency.

» Transformed a legacy organization into a modern 21st century global center of excellence. Specialized in developing and establishing maritime domain awareness safety and security systems such as the following: a maritime inland river vessel movement center tracking hazardous cargoes along America's western rivers; command and control centralization for the U.S. Nationwide Automatic Identification System; an integrated interagency global positioning system interference tracking capability; and a world-class navigation information collection and dissemination system.

» Served as C4IT System Specialist. With technical and leadership skills, maintained and operated the Coast Guard's $80M Atlantic and Gulf of Mexico's communication system for two thirds of the Coast Guard ships and aircraft, and consolidated Atlantic seaboard satellite, HF, and digital networks into Portsmouth, Virginia, during a three-year period – the most sweeping communication changes in 15 years. Led Coast Guard Y2K communication efforts to ensure no communication problems arose, which was fully successful in both planning and execution.

- Jointly designed, built, and installed Exxon Valdez oil spill clean-up communication system/network.

- Served as project lead (with engineering and operational team of experts) in designing and building a prototype for the Coast Guard's integrated buoy positioning system, which is employed today.

Publications and Presentations

- 2014 Mideast LAMPAC Conference, Speaker, "Physical Security," August 13, 2014.

- National Nuclear Security Conference, Speaker, June 18, 2014.

- First Reliability, "Critical Infrastructure Protection (GridEx II, Physical Security)," Speaker, May 21, 2014.

- Texas RE (Public Session), "GridEx II Security Exercise," Speaker, April 22, 2014.

- Grid Security Exercise (GridEx II) After-Action Report, March 2014, (NERC Program Sponsor).

- Law Seminars International, Cybersecurity Law and Strategies, "Challenges and Solutions: Lessons from Efforts to Secure Electric Infrastructure and Grid Operation," Speaker, January 28, 2014.

- GridEx 2013 Distributed Play and Executive Table Top Exercise (NERC Program Sponsor and Speaker).

- CIPC Physical Security Subcommittee, NTAS Guideline Update, Security Guideline for the Electricity Sub-Sector: Physical Security Response, Approved by CIPC on October 28, 2013 (NERC Program Sponsor).

- GridSecCon 2013 (NERC Program Sponsor).

- Northeastern University George J. Kostas Research Institute for Homeland Security, "After Hurricane Sandy: Lessons Learned for Bolstering Energy Resilience," September 17, 2013 (Speaker and Participant).

- Bipartisan Policy Center Cyber Security Event, Washington, DC, Member of Panel, August 6, 2013.

- Puget Sound Energy (PSE), Physical Security Speaker, July 2013.

- 2013 Aspen Institute Global Energy Forum, "Innovation in Electricity," July 4-7, 2013 (Speaker and security guest participant).

- Recommendations for Improving Information Sharing, CIPC Electricity Sector Information Sharing Task Force, May 2013 (Matt Blizard, NERC Program Sponsor).
- Personnel Security Clearance Task Force (PSCTF) Report, CIPC Approved on June 11, 2013 (NERC Program Sponsor).
- Northwest Public Power Association 73rd Annual Conference and Membership Meeting, Public Power: Examining the Responsibility to Serve, May 22, 2013, "Examining the Responsibility of Cyber Security," (Speaker).
- GridSecCon 2012 (NERC Program Sponsor).
- Electricity Sub-Sector Coordinating Council, Council Charter, Amended and Board Approved, August 2012 (Matt Blizard, ESCC Secretary).
- CIPC Physical Security Subcommittee, NTAS Guideline Update, Security Guideline for the Electricity Sub-Sector: Physical Security, Approved by CIPC on June 20, 2012 (NERC Program Sponsor).
- U.S. Department of Energy, "Electricity Subsector Cybersecurity Risk Management Process," May 2012 (NERC Program Sponsor).
- CIPC "Severe Impact Resilience: Considerations and Recommendations," NERC Board of Trustees, Accepted: May 9, 2012 (NERC Program Sponsor).
- CIPC "Cyber Attack Task Force, Final Report," NERC Board of Trustees, Accepted: May 9, 2012(NERC Program Sponsor).