Jonathan Trimble

Austin, Texas (703) 304-4470
jonathan.trimble@bawn.com • linkedin.com/in/jon-trimble

Executive Summary

A Senior Security Executive with 20+ years demonstrated success in information security and technology. Specialties include Cybersecurity, Intelligence and Security Operations, Information Technology, and IT Security Controls. A skilled mentor and manager, providing collaborative leadership and mentoring to multi-disciplinary teams. Adept at identifying best practices and developing solutions to driving organizational initiatives for leap ahead gains for the enterprise.

- Managed $220M Central Records Center development, saving $15M and reducing risk by 30%
- Led deployment of first FBI cloud application to support secure access to intelligence holdings
- Led development of FBI's enterprise intelligence analysis system, increasing analytic and information sharing capabilities of 38,000 employees
- Led engagement with public interest group/industry association to develop technology policies, including common security controls for government cloud environments

Professional Experience

Bawn, Austin, TX
Chief Executive Officer, 2020 - Present

Bawn is a cybersecurity provider servicing the Legal, CPA, and Private Equity communities. Leads strategy, business planning, service line development, and resource development efforts. Oversees client engagements providing cybersecurity risk assessments as well as cyber strategies and solutions that include personnel training, process development, technology configurations, and insurance packages to significantly reduce clients' cyber risk.

Praetorian, Austin, TX
Vice President of Services, 2020

Praetorian is a fast-growing cybersecurity provider. Jonathan provided direct leadership to approximately 70% of company personnel. Led strategy, business planning, service line development, and resource development efforts. Oversaw client engagements providing cybersecurity risk assessments as well as product and network security vulnerability assessments to Fortune 500 clients in healthcare, finance, and technology verticals.

- **P & L:** Exceeded revenue goals, **enabling a 22.5% YoY growth to an $18M annual revenue goal**
- **Customer Service:** Oversaw customer service record for company with **93% Net Promoter Score and 73% response rate**.

Federal Bureau of Investigation, Information Management Division, Washington, D.C.
Chief Technology and Innovation Officer (Senior Executive Service), 2018 - 2020

FBI IMD manages the agency's record and information lifecycle, organizing the information and making it appropriately accessible to both government and public entities. Promoted into a newly formed executive role to reinvigorate the division's systems and business processes. Antiquated IT systems and overly complex business processes led to an increasing backlog of information requests and elevated risk. Built the transformation strategy for the first 30 days and led execution over 90 days. Developed mission, metrics, new tools and techniques, timelines, and concepts of operations. Instituted innovation culture to inspire employees to collaborate and embrace teamwork:

- **Collaboration at Scale:** Led development of new FBI Central Records Center, a $220M construction and IT project to manage and protect FBI's core information holdings. Developed enterprise risk management strategy, established processes and workgroups and secured C-suite and senior stakeholder support to encourage enterprise-wide coordination and ensure timely delivery.
- **System Integration:** Developed risk management strategy, established processes and provided presentation updates to ensure timely delivery. **Led negotiation of critical system components, including system analysis, the configuration of APIs, system and security control documentation, and implementation of automated warehouse system.**
- **Threat Intelligence Strategy:** Led the development of a threat intelligence picture regarding the FBI's most complex project, employing a myriad of government resources. Utilized this actionable intelligence to guide new IT infrastructure design and software maintenance protocols.
- **Data Migration Planning:** Commissioned to develop IT strategy and cloud data migration plan to support the CRC development. Secured Chief Information Officer support, personnel, and funding to build a development team. Oversaw migration of critical system from Oracle to SQL platform. **This reduced risk of poor system integration, enriched planning, incorporated a cloud computing environment and provided a more reliable system.**
- **Supply Chain Security:** Utilized intelligence sources to identify possible significant security vulnerability. Coordinated assessment of affected systems, internal audit of logs and user activities, and vulnerability scans. **Developed risk mitigation strategy, which precluded a six-month delay of a major project.**
- **Change Management:** Led process improvement for multiple organizations. Managed development of standard operating procedures and corresponding management system to support continuous process improvement. Developed policy guidance and established a task force to maximize the impact of field preparation efforts. **This supported the workforce transformation of 300+ employees.**
- **Public Policy Compliance:** Built and updated the FBI's Freedom of Information Act (FOIA) Data Processing System (FDPS) (an 18-year-old technology) to achieve public policy and legal compliance and efficient processing of an increasing number of FOIA requests. Coordinated requirements development and documentation, outlined the product roadmap, and incorporated AI tech to redact sensitive information. **Delivered the RFP in a record 60 days, allowing obligation of funds to contract for replacing the system in FY18, and saving $8.7M development funding.**
- **Vendor Management/Procurement:** Acted as a key point of contact for major software development contracts exceeding $20M. Managed $16M acquisition of new infrastructure software and hardware. Developed timeline for deployment of networking and computer hardware, office software, and technical support. Monitored work performance and billing of supporting vendors.

Federal Bureau of Investigation, Norfolk, VA

Assistant Special Agent in Charge, 2014 - 2018

FBI Norfolk coordinates with the largest concentration of military commands in the country. As second in command, led the turnaround of the worst-performing Field Office (out of 56) after multiple failed turnaround attempts. Identified personnel performance, technology, compliance issues. Reinstituted mandatory training, restored reporting timeliness, and reinvigorated compliance council. **These efforts skyrocketed Performance, and within 100 days, the Norfolk Field Office achieved the #2 ranking (out of 56).** Managed FBI Cybersecurity, Network Management, and Computer Science programs, including incident response and forensics.

- **Cyber Program Management:** Tasked by Cyber Division leadership to lead key programs. Developed a plan and selected candidates for vacant positions. Redefined duties and responsibilities, reducing thresholds of responsibility and decision-making to underutilized employees. Mentored employees and encouraged more prominent leadership roles, which improved morale. **Within 30 days, achieved more effective use of personnel and management of FBI Cyber programs.**
- **Enterprise Information Security / Training:** Recruited by leadership to improve cybersecurity in major U.S. maritime, rail, and aviation ports. Conducted security risk assessment and developed security policies incorporating NIST and ISO 27001 frameworks while accounting for complex regulations. Created forum to educate 300+ private/public entities on the information security issues and provide resources for resilient network management. **This strategy was declared a Best Practice and replicated at other U.S. ports.**
- **Technology Policy Development:** Selected by C-Suite to conduct research of over the horizon technology trends. Identified industry experts and led the development of a research plan. **Resulted in security policy creation for operations use of mobile and social media technology.**
- **Business Resilience / Crisis Management:** Hurricane Dennis was headed for Hampton Roads, threatening large-scale damage to the area. Took the initiative to implement the Norfolk FO Hurricane response plan. Led office, staff, and family preparations. Coordinated efforts of neighboring field offices and the Critical Incident Response Group. Monitored employee status and directed resources to recovery efforts. **This ensured the safety of all Norfolk FO employees.**
- **Team Development / Mentoring / Coaching:** An unusually large number of IT user complaints resulted from outdated policies and await failure management strategy. Proposed solution and executed a new plan over 60 days that instituted routine checks. Established a central hotline for IT ticket issues and mentored department staff on customer engagement. **Complaints diminished to near zero, and complications during major training & operational events were eliminated.**

Federal Bureau of Investigation, Baltimore, MD

Field Supervisor, 2010 - 2014

FBI Baltimore addresses one of the highest concentrations of violent crime in the country while also addressing a wide variety of national security matters.

- **Threat Intelligence:** Promoted to address the increasing violence, drug channels, and gang activity in Prince George's County/Northeast DC. Developed "push-pull" threat intelligence model, significantly increasing impact of operations and decreasing violence by 51% within one year, immediately exceeding expectations in lowering crime levels and promoting community safety. The FBI duplicated this strategy in Oakland, CA. **Was promoted to Assistant Special Agent in Charge due to the success of this event.**

Federal Bureau of Investigation, National Security Branch, Washington D.C.

Chief, Operations Support Unit, 12/2007-05/2010

During a period of massive change post-9/11, the National Security Branch was created to oversee all FBI national security matters, including the Counterterrorism Division, Counterintelligence Division, Directorate of Intelligence, Weapons of Mass Destruction Directorate, and the Terrorist Screening Center. Commissioned by leadership to improve infrastructure and big data intelligence analytics after three years' attempts yielded substandard results. Within the year, developed and presented an assessment to all stakeholders, which demonstrated existing systems were inadequate, hindering the analytical workforce. Piloted deployment of replacement intelligence system in New York City, ingesting 2M records in 3 days. This was adopted Bureau-wide to prevent additional threats:

- **Information Security:** Resolved issues in the 2009 Google cyber-attack in days versus months.
- **Enterprise-Wide Deployment:** This system was developed to manage Counterterrorism intelligence but was later used to analyze additional data sets, including financial records, social media, etc., to address additional threats.
- **Systems Integration:** Commissioned by Executive Assistant Director to address the first-ever integration requirement between local IT systems, intelligence requirements of the FBI/Intelligence community, and a separate system that handles sensitive source reporting. Negotiated for API integration while defining processes to resolve future conflicts. **Data entry processes were reduced by 15% (~8,000 agents), saving time and creating effective business processes overall.**

Federal Bureau of Investigation, Counterintelligence Division, Washington, DC

Supervisory Special Agent, 2006 - 2007

The FBI Counterintelligence Division oversees all counterintelligence and counterespionage matters, coordinating operations with other intelligence agencies, field offices, and the U.S. military.

- **Security Policy & Procedure Development:** Unauthorized media disclosures jeopardized operational security for a $100M (annually) technical surveillance program. Redrafted the security policies (physical, construction, and information security), streamlining reporting processes by 80%, redistributed security management responsibilities, and obtained authorizations for new technologies. This planning allowed continued operations and intelligence gleaned continues to ensure national security. **This strategy was declared a Standard Operating Procedure.**

Federal Bureau of Investigation, Jacksonville, San Juan, and Washington Field Offices

Special Agent, 1995 – 2006

- **Electronic Surveillance/Investigation:** Discovered a check fraud scandal, in which 80 financial institutions in the U.S. lost ~$5M. Interviewed financial institutions to link stolen identities, utilized loss prevention ruse to identify and intercept subjects' phone information using new technology. This led to the identification of 3 Nigerian crime cells. Defined new legal grounds and arrested eight subjects, dismantling the criminal enterprise. **Was named an "expert" on Nigerian Organized Crime by the FBI.**

- **Cyber investigation:** Initiated and planned the strategy for an investigation of computer hackers who were located in Eastern Europe. The subjects obtained millions of credit card numbers by compromising credit processor databases, then used the information to purchase high-tech equipment, ship it overseas, then sell it on the black market. **Utilized sophisticated investigative techniques and facilitated the training of Ukrainian law enforcement, leading to the arrest of a subject-based in Estonia, identification of additional subjects in Ukraine, and increased Ukrainian law enforcement cyber expertise.**

U.S. Coast Guard, Alameda, CA and Miami, FL Commissioned Officer, 05/1990 – 10/1995

- **Electronic Systems Management:** Responsible for Combat Information and Electronic Warfare Systems onboard High Endurance Cutter. Acted as field liaison with Coast Guard Research and Development center for data link project.

Education

Master of Science: Systems Architecture & Engineering
University of Southern California (USC), Los Angeles, CA
Bachelor of Science: Marine Engineering

Master of Science: Strategic Intelligence
Carnegie Mellon University
Chief Information Security Officer

Global Information Assurance Certification (GIAC)
Information Security Fundamentals (GISF)

National Intelligence University, Washington, DC

United States Coast Guard Academy, New London, CT

Security Essentials (GSEC)
Certified Incident Handler (GCIH)
Certified Incident Analyst (GCIA)
Certified Continuous Monitoring (GMON) Certified Smartphone Forensics (GSFA)

Awards

Special Achievement: Field office compliance inspection 2018
Special Achievement: Acting Special Agent in Charge 2017
Special Achievement: Acting Chief, Cyber Ops Section I 2016
Award of Merit, Washington DC Metro Police Department: Outstanding investigation 2013
Special Achievement: Management of national security information technology systems 2008
Exceptional Performance: intelligence collection initiative 2007
Exceptional Performance: Outstanding investigation 2004
Special Achievement: Outstanding investigation 2002
FBI Director's Commendation: Outstanding investigation 1999
FBI Director's Commendation: Outstanding investigation 1997
Special Achievement: Management of national security information technology systems 2008