# Kyle M. Miller

miller_kyle@bah.com
(703) 984-1893

## Summary

As a Principal/Director at Booz Allen Hamilton, Mr. Miller oversees the firm's Operational Technology (OT) Cybersecurity practice within the Global Commercial account. He acts as an ICS/SCADA and OT/IoT cybersecurity SME to a myriad of clients, serves as technical director for internal OT/IoT investment efforts, as well as leads client delivery across a number of market areas.

With over fifteen years of professional experience, Mr. Miller has worked with a multitude of clients across the manufacturing, oil & gas, defense, energy, mining, and water/wastewater critical infrastructure sectors. These clients have included Fortune 100 and Global 2000 organizations as well as the United States Department of Defense (DoD) and other Civil agencies. Throughout this time, he has conducted security design engineering efforts, architected secure control system networks, and built-out control system focused threat detection and response programs. He has also developed service-wide and company-wide risk assessment frameworks and conducted on-site security reviews at hundreds of plants/facilities.

Mr. Miller holds an active Top Secret clearance and maintains various professional certifications including: CISSP, CEH, CHFI, GICSP, ISO 27001 Lead Auditor, Security+, and PMP. He also holds two Graduate Certificates and a Master's Degree in Cybersecurity.

## Experience

### BOOZ ALLEN HAMILTON — JUNE 2010 – PRESENT — HERNDON, VA

- **Booz Allen ICS/OT/IoT Cybersecurity – Commercial Capability Lead**
  - Oversees the OT/IoT Cybersecurity Practice within the Global Commercial account directing activities of a multi-functional team deployed across various client engagements and internal research and development activities
  - Served as a firm-wide SME in the area of OT/IoT cybersecurity and led numerous marketing, business development, and proposal efforts across a variety of markets
  - Acted as program manager overseeing multiple technical projects relating to industrial cybersecurity strategy, engineering, assessments, threat detection, and incident response
- **Pharmaceutical Manufacturing Clients (multiple) – Industrial Cybersecurity SME/Team Lead**
  - Led various teams of individuals across several major pharmaceutical industry clients performing a variety of industrial cybersecurity related tasks
  - Conducted site and organization-wide evaluations of ICS cybersecurity and architecture
  - Developed network segmentation designs for overall manufacturing processes as well as detailed Distributed Control System (DCS) segmentation architectures
  - Deployed Splunk analytics, dashboards, and reports to evaluate ICS network traffic and alert to anomalies and potentially malicious actors in the environment
- **Electrical Vehicle Automotive Client – OT/IoT Cybersecurity SME/Executive Lead**
  - Led a team of OT SMEs and cybersecurity practitioners to secure a large 3.2 million square foot EV vehicle and battery manufacturing facility from cyber threats
  - Provided SME support across multiple workstreams including OT/IoT threat detection, network segmentation, security tool evaluation, and firewall hardening
- **International Commercial Off-Shore Oil & Gas Client – ICS Assessor and Security Engineer**
  - Conducted design and engineering phase qualitative/quantitative risk assessment of 30+ ICS across four man-made island greenfield sites within the United Arab Emirates (UAE)

- Architected integrated security design recommendations and engineering packages for connections between green-field, brown-field, and corporate headquarters I-Field systems
- Designed and developed Cyber Security Management System (CSMS) and Risk Assessment Framework for one of the world's largest offshore oil fields
- Engineered integrated ICS and corporate IT Security Operations Center (SOC) design to enable cohesive understanding of organizations overall operational security posture
- Established a unified risk assessment approach and tool to assess the clients ICS assets against industry best practices including NESA, ISO 27001, and IEC 62443 standards

- **Nuclear Power Station/Fleet Clients (multiple) – Industrial Cybersecurity Engineer**
  - Conducted engineering design reviews and security assessments against plant CDAs in accordance with Nuclear Regulatory Commission (NRC) guidance and NEI 08-09
  - Developed security engineering and architecture recommendations for mitigating identified vulnerabilities as well as for new CDAs to be implemented in the plant
  - Conducted cyber remediation actions for plant Critical Digital Assets (CDAs) including developing necessary engineering change packages, drafting contingency plans, and implementing configuration changes where necessary

- **Bureau of Reclamation – Multiple sites – OT Cybersecurity SME/Team Lead**
  - Led a team of ICS engineers, cyber practitioners, and physical security specialists to conduct multiple cybersecurity assessments of several key ICS and SCADA systems, including at one of the largest power stations in North America
  - Worked with plant cybersecurity staff and engineers as well as agency cybersecurity executives to identify high risk areas and develop a plan for implementing remediations

- **EPA - Water and Wastewater Utilities – ICS/SCADA Assessment Team Lead and SME**
  - Led a team of individuals to assess ICS/SCADA systems across 50+ water treatment plants
  - Provided SME support and strategy development on 100+ additional assessments
  - Conducted on-site assessments including an evaluation of technical configurations, physical security, interviews, and a review of documentation/policies
  - Developed a custom risk assessment framework utilizing IEC 62443 and ISO 27001 standards and drafted security trend and remediation report for national publication
  - Presented overall findings and recommendations at two regional and four national conferences as well as published an industry journal article on the topic

- **Booz Allen OT Cybersecurity Lab – Chief Engineer and Lab Manager**
  - Designed, engineered, constructed, and programmed control system lab to include separate ICS and Building Control System (BCS) control system environments
  - Programmed PLCs, designed HMIs, and configured wired/wireless industrial networking

- **EPA Water Security Division – ICS Security Training and Incident Response Exercise Lead**
  - Conducted 30+ cybersecurity trainings at a variety of locations across the U.S. targeting water/wastewater sector operators, plant managers, and executives
  - Developed course curriculum and training materials covering the topics of: cybersecurity threats, standards, tools, and best practices for securing ICS/SCADA systems
  - Facilitated incident response scenarios describing an attack on both the IT business networks as well as the SCADA systems of a fictitious water utility

- **International Commercial On-Shore Oil & Gas Client – Risk Assessor**
  - Conducted a full-scale risk and vulnerability assessment of 40+ ICS across six production oil field and pipeline sites throughout the UAE
  - Developed a risk assessment methodology and tool to assess the clients ICS assets against industry best practices including the ISO 27001 and IEC 62443 standards

- Authored primary client deliverables including a security roadmap report, risk treatment plan, manpower and organizational support model, and several policies and procedures
- Held an Abu Dhabi Critical National Infrastructure Authority Oil Field Security Clearance

- **DoD Enterprise Information Technology Directorate (EITSD) – ICS Assessment Team Lead**
  - Conducted ICS vulnerability and risk assessments across the Pentagon's critical infrastructure systems to include building control, physical access security, HVAC, CCTV, biological/radiological detection, energy management, and lift control systems
  - Provided detailed analysis and recommendations of ICS technical configurations, network design, and ICS-to-IT interconnection security

- **Air Force Civil Engineer Support Agency (AFCESA) – ICS C&A SME**
  - Consulted with AFCESA to craft the risk assessment methodology and tools used to secure service-wide Platform Information Technology (PIT) ICS
  - Identified deficiencies with client's practices and developed new streamlined processes which increased the productivity and quality of on-site ICS risk assessments by 54%
  - Designed and developed a new risk assessment methodology that is used to more efficiently gather and report data from identified risks for the 1800+ ICSs across the USAF

- **USAF Civil Engineering (A7C) – Systems Security Engineering (SSE) and C&A Team Lead**
  - Acted as team lead and job manager over five major task areas, including managing resources, staffing, hiring, scheduling, and performance management
  - Functioned as Information Assurance Manager (IAM) for the USAF service-wide geospatial GeoBase system and Information Assurance Officer (IAO) for the NexGen IT system
  - Completed full-lifecycle of C&A activities for enterprise-wide acquisition and legacy systems to obtain and retain multiple system accreditations
  - Conducted IA testing of multiple systems by running both automated and manual security tests, including DISA STIG validations and SCAP/SRR vulnerability scans
  - Contributed to the eMASS development/deployment "tiger-team" for the Air Force

## Education

**University of Maryland Global Campus – Graduate School of Management and Technology**
**M.S. Cybersecurity** **Adelphi, MD**

- Recipient of Graduate Certificate in Foundations of Cybersecurity – May 2011
- Recipient of Graduate Certificate in Cybersecurity Technology – May 2012

**George Mason University – Volgenau School of Engineering**
**B.S. Information Technology** **Fairfax, VA**

- Graduated with distinguished recognition and Latin honors
- Member of the Collegiate Cyber Defense Competition (CCDC) Team

## Industry Certifications

- Global Industrial Cyber Security Professional Certification (GICSP)
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- Computer Hacking Forensic Investigator (CHFI)
- International Standards Organization (ISO) 27001 Lead Auditor (BSI Group)
- CompTIA Security+
- Project Management Professional (PMP)


# Gemma Kite, P.E.

Senior Environmental Engineer
gkite@horsleywitten.com


**Areas of Expertise**
Environmental Engineering
Watershed Planning & Assessment
Ecological Restoration
Data Management
Water Security
Emergency Preparedness & Response
State Guidance

**Professional Registrations & Affiliations**
Professional Engineer, MA
Member, New England Water Environment Association (NEWEA)
Member, Water Environment Federation
Member, Engineers without Borders

**Academic Background**
Masters of Engineering, Biological and Environmental Engineering, Cornell University
Bachelor of Science, Environmental Engineering, Lehigh University

**Professional Experience**
Horsley Witten Group, Inc., Senior Environmental Engineer, October 2013 to Present
Inter Aide, Water and Sanitation Program Manager, 2011 to July 2013
Langan Engineering, Engineering Intern, 2008

**Publications**
Kite, Gemma, Summer 2011. ClearWaters. New York Water Environment Association, Inc. "Water Politics in a Rural Malian Village."

Horsley Witten Group
*Sustainable Environmental Solutions*

Gemma Kite is a registered professional engineer in Massachusetts with more than ten years of professional experience as an environmental engineer specializing in emergency preparedness training, state guidance development, hydrogeologic investigations and modeling, and watershed planning and assessment. As a senior environmental engineer with the Horsley Witten Group, Inc. (HW) Ms. Kite works on a variety of projects including assisting states and EPA with developing program guidance, developing and presenting material for water security trainings for the water sector, and conducting environmental site assessments. Prior to HW, Gemma worked in Sierra Leone and Mali as a Water and Sanitation Program Manager for a French non-governmental organization, specializing in water security issues.

## KEY PROJECTS

***Water Sector Cybersecurity Technical Assistance:*** Gemma is supporting EPA in providing free, confidential, cybersecurity assessments and technical assistance to interested water and wastewater utilities. Participating utilities will be provided technical assistance to implement best practices to better prepare for, respond to, and recover from cyber incidents. The technical assistance provides a customized Cyber Action Plan that contains the recommended best practices for the utility to implement based on the assessment. The assessment and technical assistance cover cybersecurity for both business enterprise systems and industrial control systems (e.g., SCADA). To date, the project has assessed over 100 utilities across the country. Gemma has served as the project manager since 2019.

***Water Sector Cybersecurity Introduction Workshops:*** ***T***o further increase utility resilience, Gemma assisted EPA to develop and conduct free, one-day cybersecurity workshops and response exercises throughout the United States. The workshops are intended to teach water and wastewater utilities more about the cyber threat, ways to manage the threat, and tools available to help utilities. In addition, results from Virginia waterworks cyber assessments are presented to share lessons learned. Facilitated response exercises are conducted presenting realistic cyber threat scenarios, allowing all participants to discuss the actions they would take in response to the threat. The goal of the exercises is to identify general planning or procedural actions that enhance cybersecurity and mitigate risk. Gemma developed multiple training presentations designed to instruct utilities on the cybersecurity threat overview, regulatory guidance and standards, and available tools, resources and methods to achieve enhanced resiliency. Gemma updates the workshop presentation materials each year to reflect changes in threats, guidance, and available tools. Gemma has facilitated these workshops since 2015.

***AWWA Water Sector Cybersecurity Risk Management Tool Training Materials:*** Gemma assisted AWWA with the development of eLearning and in-person workshop materials to train users on the use of the AWWA's Water Sector Cybersecurity Risk Management Tool, released in September 2019. The updated version of the tool helps facilitate compliance with America's Water Infrastructure Act of 2018. Gemma developed five modules on how the tool works and how to use the tool, as well as corresponding workshop materials like the instructor's guide.

***Cybersecurity Assessments of Drinking Water Utilities in Virginia and Development of Technical Materials:*** Under the direction of EPA Region 3 and the Virginia Department of Health (VDH), Gemma assisted to complete multiple on-site cyber security assessments of Virginia water utilities' SCADA and

business computer systems. For the assessments, Gemma coordinated with a subcontractor to visit each site and conduct an interview- and inspection-based assessment to gain an understanding of the state of cyber practices. Utility participants included representatives from IT and automation staff. Summary tables and charts were developed presenting the results of each utility assessment, and overall trends and patterns were identified across all participating utilities to allow for statewide analyses and information sharing. Based on the aggregated results of the assessments, Gemma developed materials for both VDH and Virginia utilities with the goal of improving the cyber resiliency/security. The materials provide effective and affordable solutions to improving cybersecurity. The overarching goal of the program is to empower utilities with the knowledge to improve their utility's cyber resiliency/security using low or no cost techniques.

***Cybersecurity Checklist and Table Top Exercise Tool:*** On behalf of EPA, Gemma developed the Cybersecurity Incident Action Checklist, which provides water and wastewater utilities with actions for preparing for, responding to, and recovering from cybersecurity incidents. The checklist was based on information provided during the water sector cybersecurity workshop series, as well as information from other security agencies, like Department of Homeland Security. In addition, Gemma also adapted the two response exercises from the cybersecurity workshop series into one exercise to be included in EPA's Tabletop Exercise Tool for Drinking Water and Wastewater Utilities as a cyber scenario. The tool provides users with the resources and documents to plan, conduct, and evaluate exercises. Gemma developed the presentation, situation manual, planning documents, and after-action report for the cyber scenario. The documents are fully customizable to fit the utility's needs and situation.

***Wastewater Operation, Maintenance and Management Training for Rural Communities – EPA Office of Wastewater Management:*** Gemma assisted EPA in facilitating multiple training for small and rural communities across the country on wastewater system operations and maintenance and effective techniques to operate a sustainable utility. Gemma presented several topics related to utility operation and maintenance and facilitated small group discussions. In addition, Gemma tailored training materials to be location specific and to reflect updated technology information. Materials include presentations with speaker notes and exercises for participants.

# Jesse Stewart
# Booz Allen Hamilton
Stewart_Jesse@bah.com, **(215) 801-6837**


**EDUCATION:**

| | | | |
|---|---|---|---|
| BS | The Pennsylvania State University | Security & Risk Analysis; Information & Cyber Security | Dec/2010 |
| | | Minor: Information Sciences and Technology | Dec/2010 |

**EMPLOYMENT HISTORY:**

| | | | |
|---|---|---|---|
| Booz Allen Hamilton | Branchburg, NJ | 2018 – Current | Associate |
| Booz Allen Hamilton | New Hill, NC | 2014 – 2018 | Associate |
| Booz Allen Hamilton | Colorado Springs, CO | 2012 – 2014 | Sr. Consultant |
| Booz Allen Hamilton | Washington D.C. | 2012 – 2012 | Sr. Consultant |
| High Performance Technologies, Inc. | Washington D.C. | 2011 – 2012 | Risk Analyst |

**KEY SKILL AREAS:**

- Operational Technology
- Certification and Accreditation
- Information Security
- Risk Assessment
- Cyber Security
- Program and Project Management
- Network Segmentation
- Risk Mitigation
- NEI 08-09
- NIST 800-53

**CERTIFICATIONS:**

Security+ (CompTIA)
INFOSEC NSTISSI 4011

**CLEARANCE:**

Cleared for Top Secret based on a single scope background investigation completed on 3 March 2011
Previously Nuclear badged and a member of the critical group

**EXPERIENCE SUMMARY:**

Mr. Jesse Stewart is a Booz Allen Associate with over 10 years of Cyber Security experience that spans Information Technology (IT) and Operational Technology (OT) in both Commercial and Government sectors. He brings both team and project lead experience and has technical knowledge of many IT and OT tools and concepts. Jesse has facilitated the development and execution of firewall hardening and network segmentation for a large global pharmaceutical manufacturing company through comprehensive review and development of firewall rules and shopfloor network designs. Jesse has performed cyber security compliance assessments for NEI 08-09, NEI 13-10 and NIST 800.53 based controls and has extensive knowledge and experience with numerous assessment methodologies including the Risk Management Framework (RMF), DoD Information Assurance Certification and Accreditation Process (DIACAP), and the EPRI Technical Assessment Methodology (TAM). Achieving an advance Cyber Security Specialist certification from his client, Jesse was responsible for leading a Cyber Security Assessment Team (CSAT) to approve remediation and mitigation actions for Engineering Change packages and Milestone 8 assessments on ICS equipment at an East Coast Nuclear Power Plant. His previous work has included supporting certification and accreditation efforts for DoD systems, as well as contributing to Computer Incident Response Teams (CIRT) via response, tracking, documenting, and mitigation of identified cyber incidents and potential threats. Furthermore, he has a Bachelor of Science in Security and Risk Analysis from The Pennsylvania State University with a minor in Information Sciences and Technology. Over the years he has held, Certified Ethical Hacker, Security+ (CompTIA), and INFOSEC NSTISSI 4011 certifications. Jesse has an active Secret security clearance and is Top Secret eligible.

**EXPERIENCE:**

**Booz Allen Hamilton** **August 2012 – Present**

***Associate– Global Pharmaceutical Company (Branchburg, NJ, May 2018 – Current)***

- Improved the Cyber Security posture of more than 30 global pharmaceutical manufacturing plants through development of zero-trust firewall rules and physical and logical network segmentation.
- Utilized tools such as Cisco Security Manager, Splunk, Tufin, and Stealth Watch to capture and analyze observed network traffic through key network devices and use that information to craft firewall rules and logical boundaries for communication with end devices.
- Facilitated informational meetings with manufacturing shop floor leaders highlighting the importance of security between Informational Technologies (IT) and Operational Technologies (OT) and opened dialog about site specific concerns and plans.
- Investigated unexpected traffic seen in Splunk logs to determine how/where traffic was circumventing existing firewall rules and proposed new rules or rule modification.

***Associate– Shearon Harris Nuclear Power Plant (New Hill, NC, November 2014 – Dec. 2017)***

- Obtained an advanced certification, Cyber Security Specialist (CSS), and was responsible for cyber security evaluation of all Engineering Change (ECs) requests for nuclear plant systems (e.g. ERFIS, Plant Fire Protection and Detection Systems, EPNET, Security Diesel Generator, Met Tower, TSC HVAC, etc.).
- Facilitated cyber security reviews for over 140 plant systems and provided security posture and mitigation actions in accordance with 10 CRF 73.54, NEI 08-09, NEI 13-10, and Security Control and Implementation Strategy (SCIS) to ensure the client would surpass their regulatory compliance commitments for Milestone 8.
- Conducted gap analysis to identify, validate, and help mitigate system risks and vulnerabilities for industrial control systems through the compilation of asset walkdowns and risk and vulnerability assessments
- Performed identification and evaluation of Critical Digital Assets (CDA) and Critical Systems (CS) as part of Milestone 2 efforts.

***IA Analyst– Headquarters Air Force Space Command A6 (Peterson AFB, CO, June 2013 – Nov. 2014)***

- Evaluate the security posture of network enclaves, information systems, and Automated Information System (AIS) applications on the Air Force Network (AFNET).
- Identify, validate, and help mitigate system risks and vulnerabilities in order to assist government Action Officers (AO) in providing accreditation determination recommendations to the Air Force Certifying Authority (CA) and Designated Approving Authority (DAA).
- Complete risk and vulnerability assessments to identify specific system risks and potential risks to the AFNET and other connected systems.
- Assist with the development and presentation of training briefings for the transition to Risk Management Framework (RMF) from Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).

***IA Analyst – Defense Civilian Personnel Advisory Services* (Mark Center, VA, April 2013 – June 2013*)***

- Conducted certification and accreditation (DIACAP) and patch management activities for DoD systems.
- Utilized eEye Retina and Vulnerator to complete network scans and generate vulnerability reports for release to the system administrators.
- Reviewed POA&M and DIACAP package documentation as well as assist with the developed of SOPs for vulnerability management and continuous monitoring.
- Conducted interviews of developers, vendors, and system administrators to gather security information
- Responded to, tracked, and mitigated incidents as identified by the Pentagon Computer Incident Response Team (PENCIRT).

*Information Assurance Analyst – MBW (Navy Yard, DC, February 2013 – April 2013)*

- Assisted with running network scans and generating vulnerability reports utilizing eEye Retina.
- Presented internal audit scan findings and made recommendations for improving the current network security posture to the clients' senior management.

*Local Registration Authority – Army CIO/G6 (Fort Belvoir, VA, December 2012 – February 2013)*

- Interfaced with various government representatives to ensure successful localized implementation and integration of the ASCL/NSS tokens.
- Utilized CIW and Active Directory to manage user certificates on NIPRnet and SIPRnet user tokens and ensure seamless functionality for the recipient of the tokens.
- Successfully managed logistics and accounting capability for the largest CCSA roll out of the NSS SIPR technology.
- Assisted with the development of reports to track the progress of the LRAs and RAs for the client.

*Senior Consultant (McLean, VA, August 2012 – December 2012)*

- Assisted with the development of the hands-on virtual cyber security training lab that will be used to educate new hires and employees through hands-on training with the most commonly used tools.

**High Performance Technologies, Inc. Arlington, VA January 2011 – August 2012**

*Risk Analyst – The Department of Veterans Affairs (February 2012 – August 2012)*

- Facilitated, lead, and drove reoccurring risk and issue meetings with VA leadership, maintaining direct correspondence with the client in order to keep the risk and issue logs up to date at all times.
- Managed risk and issue logs by identifying, logging, and tracking risk and issues from identification to close.
- Communicated the risks and issues as they evolved to the client to ensure that they had the most up to date information about potential impacts to their projects.

*Support Specialist – The Department of Veterans Affairs (January 2011 – February 2012)*

- Developed and reviewed Risk Management Framework (RMF) C&A deliverables including Privacy Impact Assessment and System Security Plan using standards as outlined in the NIST Special Publications.
- Supported the certification of General Support Systems (GSS) and Major Applications through development of required deliverables and monitoring and tracking the Plan of Actions and Milestones (POA&M).
- Worked to develop a recruitment program in the form of a problem solving competition that was then deployed at both the Pennsylvania State University and James Madison University.