

EXHIBIT 1

Jason B. Lyons

13829 233rd CT NE
Woodinville WA, 98077

SUMMARY

Jason Lyons is an experienced investigator specializing in computer investigations. Trained and experienced in hacker methodology/techniques, computer forensics, incident response, electronic discovery, litigation support and network intrusion investigations.

SECURITY CLEARANCE

- Top Secret/SCI-Expired.

CERTIFICATIONS

- Encase Certified Examiner (EnCE) - Guidance Software
- Sans Certified Incident Handler (GCIH)-SANS
- Counterintelligence Special Agent - Department of the Army
- Certified Basic Digital Media Collector - Department of Defense
- Certified Basic Computer Crime Investigator – Department of Defense
- Certified Basic Digital Forensic Examiner – Department of Defense
- State of Texas licensed Private Investigator

TECHNICAL SKILLS

- Network Intrusion Investigations
- Incident Response
- Investigative Network Monitoring
- Investigation Management/Liaison
- Computer Media Evidence Collection
- Computer Forensics
- EnCase Certified Examiner
- PDA and Cell Phone Seizure and Forensics
- Expert Witness Experience
- Technical/Investigative Report Writing

PROFESSIONAL EXPERIENCE

2013-Present *Microsoft Digital Crimes Unit (DCU)*
Senior Manager of Investigations

2012 – 2013 *Xerox Information Security Office*
Director of Forensics, eDiscovery and Incident Response

- Responsible for investigating, reporting, and responding to information security incidents worldwide.
- Manages an incident team who utilizes various forensic techniques to investigate information security incidents to include computer forensics, log analysis, network forensics, Intrusion Detection System (IDS) alerts, and malware analysis.
- Developed threat and risk matrices based on incidents types and report findings to upper management.
- Developed processes and procedures based on incident alerting sources, including escalated IDS alerts, MacAfee EPO, Email Spam filters, and Data Loss Prevention (DLP) alerts.

Works with multiple vendors to develop proactive Proofs of Concepts (POC) to increase the company's security posture.

- Responsible for managing, coordinating, investigating, and reporting on legal, corporate security, human resources, and ethics investigations involving digital media.

2012-2012 ***Xerox Information Security Office
Cyber Intelligence Response Team (CIRT)
Manager of the CIRT***

- Manager of the Cyber Intelligence Response Team (CIRT) for a fortune 500 company. Responsible for investigating, reporting, and responding to information security incidents worldwide.
- Manages an incident team who utilizes various forensic techniques to investigate information security incidents to include computer forensics, log analysis, network forensics, Intrusion Detection System (IDS) alerts, and malware analysis.
- Developed threat and risk matrices based on incidents types and report findings to upper management.
- Developed processes and procedures based on incident alerting sources, including escalated IDS alerts, MacAfee EPO, Email Spam filters, and Data Loss Prevention (DLP) alerts.
- Works with multiple vendors to develop proactive Proofs of Concepts (POC) to increase the company's security posture.

2005 – 2011 ***Affiliated Computer Services, inc (ACS)/Xerox
Digital Forensic, eDiscovery Group
Manager of the Digital Forensics Group (DFG)***

- Manager of a fortune 500 company's digital forensic laboratory/group. Responsible for managing, coordinating, investigating, and reporting on legal, corporate security, human resources, and ethics investigations involving digital media.
- Developed policy and procedures for digital evidence acquisition, storage, examination, processing and production.
- Developed and maintained technical investigative support for ACS inside and outside legal counsel on eDiscovery matters. Experienced in developing and executing large eDiscovery collection plans, preserving data in a forensically sound manner, culling of relevant data, presenting data for review, hosting data for review, and producing relevant data for final production.
- Implemented Access Data's Enterprise and eDiscovery solution.

2003 – 2005 ***Department of the Army, 902nd Military Intelligence (MI),
Cyber Counterintelligence Activity (CCA)
Assistant Operations Officer/Counterintelligence Special Agent***

- Assisted in managing of all CCA branch operations to include all cyber investigations, special intelligence collection missions, cyber investigator training, and quality assurance of all investigative products.
- Supervised 35 special agents and computer forensic technicians.
- Prepared detailed investigative briefings which include results of investigations and forensic analysis for executive level officers.
- Conducted national level liaisons with federal intelligence and law enforcement agencies on many national security investigations.
- Conducted network intrusion investigations, computer media forensics examinations, counterintelligence/counterterrorism special operations, and network forensic analysis.

2000 – 2003 ***Department of the Army, 902nd MI, CCA***
Counterintelligence Special Agent / Computer Investigator

- Assistant Supervisory Special Agent (ASSA) of an eight man computer Incident Response Team (IRT) specializing in cyber investigations.
- Accountable for managing, editing and reviewing associated technical and investigative reports pertaining to the IRT's investigations.
- Provided and maintained incident response, computer forensics, evidence handling, and computer media search and seizure training for the members of the IRT.
- While assigned to the IRT, served as lead agent on numerous network intrusion and computer forensic Counterintelligence investigations.

1998-1999 ***Department of the Army, 501st MI Brigade, South Korea***
Counterintelligence Special Agent / Liaison Officer

- Served as liaison officer for a Counterintelligence Resident Office in South Korea.
- Maintained regional-level liaison with foreign government officials to collect strategic information for intelligence reporting.
- Established business partnerships and furthered cooperation between the United States and South Korean investigative/intelligence agencies to accomplish bilateral goals.

EDUCATION

- Graduate from Excelsior College in October 2002, with a Bachelor of Science in Liberal Arts.
- Thirteen hours completed for Masters Degree in Information Technology with University of Maryland University College (UMUC).

TRAINING

- Counterintelligence Agent Course-Department of the Army-1998.
- Counterintelligence Fundamentals Warfare (CIFIW)-Department of the Army-2000.
- Introduction to Computer Search and Seizure-Defense Computer Investigation Training Program (DCITP), Linthicum, MD-2000.
- Introduction to Networks and Computer Hardware (INCH)-DCITP, Linthicum, MD-2000.
- Network Intrusion Analysis Course (NIAC)-DCITP, Linthicum, MD-2001.
- Computer Investigations for Special Agents (CICSA)-Department of the Army-2001.
- Basic Evidence Recovery Techniques (BERT)-DCITP, Linthicum, MD- 2002.
- Basic Forensic Examiner Course (BFE)-DCITP-Linthicum, MD-2002.
- Forensics in a Solaris Environment (FISE)-DCITP-Linthicum, MD-2002.
- SANS-Tracking Hackers/Honey pots-SANS Institute, Dupont Circle, DC-2003.

- Encase Intermediate Analysis and Reporting-Guidance Software, Sterling VA-2004.
- PDA and Cell Phone Seizure and Analysis-Paraben Software, Orlando FL-2005
- Network Monitoring Course (NMC)-DCITP- Linthicum, MD-2005
- Encase Advanced Internet Examinations-Guidance Software, Los Angeles CA-2006
- (FTK) Windows Forensics-AccessData, Dallas TX-2006
- (DNA) Applied Decryption-AccessData, Nashville TN, 2007
- Network Intrusion Course-Guidance Software, Houston, TX, 2010
- SANS-Hacker Techniques, Exploits, and Incident Handling, San Francisco, CA, 2011