EXHIBIT 1.1

Doug Gould, CISSP, CAS

Doug Gould is a results-oriented security leader with 35YRs+ experience in Business and Government Solutions security services. He has successfully partnered with management and technical leads of global corporations and government organizations to design solutions, demonstrate and implement technical capabilities of security products and services, and advise C Level clients as a Chief Security Strategist while at AT&T. Doug is currently the Chief Technical Officer at Cyber Team US.

CORE COMPETENCIES

- Business Management
- Security Architecture & Design
- High Level and Detailed Security Policy
- Security Infrastructure: FW, IDS, IPS, and more
- Systems Security –Unix/Linux & Windows
- Regulatory Compliance - SOX, HIPAA, more
- Penetration Testing and Assessment (IT Security, also Physical Security)
- Rationalization of GRC and Risk Management
- Physical Security - Threat Assessment/Risk Analysis; TSCM; Protection Strategy; Design
- Public Key Infrastructure; AAA solutions
- Enterprise Systems Administration; Infrastructure-wide Config Management
- Bus. Continuity Planning, Disaster Recovery
- SCADA, Process Control, Pharmaceutical compliance (21 CFR & cGxP's)
- Security Investigation, Computer Forensic Expert

PROFESSIONAL EXPERIENCE

- Chief Technical Officer, and 50% owner, Cyber Team US
- Chief Security Strategist, AT&T Security Center of Excellence
- Technical Security Consultant, AT&T Security Center of Excellence
- Principal Security Architect, City and County of San Francisco (Health Information Exchange, leading national standards initiatives)
- Principal Security Architect, State of Florida enterprise network (OC core MPLS network, 4000+ CPE routers, advanced security); planning, design and implementation.
- Advanced Convergence Secure VPN Infrastructure development and deployment
- Commercialization Implementation team, AT&T's global-scope Aurora SIEM platform
- Appointed Chief Information Security Officer, World Institute for Security Enhancement.
- Forensic Analyst, Expert Witness*
- Senior Faculty Member, World Institute for Security Enhancement – Computer Forensic Analysis, Advanced Computer Forensic Analysis, Technical Surveillance Countermeasures.
- Instructor, Checkpoint Firewall-1 NG with AI
- Advanced SIEM Architecture Design & Implementation (Cisco MARS, Q-Radar, Intellitactics, others)
- Firewall and Network Security in HA Extreme Criticality National Security Government / DoD environments

- Multi Vendor VPN Interoperability Specialist
- Author, *Information Security Framework Methodology*TM
- Principal Security Consultant, Able Information Security – Checkpoint, Symantec, Cisco and Forensic expert
- Course Author & Instructor, *Beyond CISSP, Advanced Computer Forensic Analysis*
- Senior Computer Forensic Analyst, *Expert Witness*
- **Keynote Speaker, Able 2004 Security Conference –** *Norfolk Virginia, "The Future of Computer Security".*
- Physical and Electronic Security Assessment for Federal Critical Infrastructure Data Centers
- President, Eastern Carolina InfraGard, 2002-2003
- Performed Security Audits, Security Assessments and Penetration Testing
- Installed and Configured ASA, PIX, FWSM and Checkpoint firewalls and, Checkpoint Interspect, Symantec Manhunt, Cisco IDS, Enterprise Security Manager (ESM), Silent Runner, more …
- Installed and Configured High Availability and Load Balancing Firewall Solutions supporting VPN access for >16,000 simultaneous global (worldwide) users in DoD environments
- Performed Firewall Installation, configuration, rule base and policy development for Federal, State and Local Governments, and for National Critical Infrastructure organizations (US Ports), as well as numerous commercial clients
- Established Multi-Vendor Interoperability VPN Solutions, including leading edge secure Converged Services
- Consulted with clients on, developed and authored corporate security policies.
- Architected 900-node international business network and operational security infrastructure
- Performed Regulatory Compliance assessments for computer security, authentication and electronic signatures in regulated environments
- Performed assessment against Sarbanes-Oxley, HIPAA, PCI, ISO-17799, NIST Standards, FISMA, FIPS, DOE Criteria, DoD STIG's, FERC and NERC guidelines.
- Expert in security of SCADA (Supervisory Control And Data Acquisition) systems and networks
- Performed Application Security Assessments for Database Systems, Manufacturing Systems and Control Systems in regulated environments

Current Position – *Chief Technical Officer, Cyber Team US*
Responsible for operations management including service delivery, sales force management, consulting services, training, operational infrastructure design, implementation and business management, business strategy, marketing and growth strategies.

Previous Experience – *Senior Technical Security Consultant, AT&T Security Center of Excellence*
Upon AT&T acquisition of Alienvault, AT&T Cybersecurity was formed. I have been a key person in the development of security messaging in the new AT&T Cybersecurity business unit. Key spokesperson for AT&T Security offers – presenting and demonstrating AT&T offers to customer cabinet-level officers. Core ability to simplify technology and present key advantages in a business leadership context. Uniquely able to translate technological advantage into business imperative. Retired from AT&T in 2020.

Previous Experience – *AT&T Chief Security Strategist*
Responsible for leading security strategy for all of AT&T's Enterprise and Global Transnational customers. As one of the most senior Subject Matter Experts (SME) in information security, worked with chief executives and cabinet officers of the Fortune-500 and Global Transnational companies to define approaches to address comprehensive security concerns from strategic alignment of risk and compliance with business goals to specific integration of solutions into existing infrastructures defining a path of continuous improvement toward the ultimate goal of achieving desired risk tolerance. Led a team of SMEs and Application Security Executives to achieve sales objectives. Facilitated Product management and operations collaboration to strengthen the portfolio and improve market position. Managed large complex projects including difficult client retention and account recovery strategies with a well-reasoned and disciplined approach, a can-do attitude and drive to get things done.

Previous Experience – *Principal Architect, Security, AT&T*
In this role defined security implementations for large corporations, US States and the US Federal Government, from high level strategy to detailed design. Defined Governance, Risk and Compliance for multiple clients in conjunction with security architecture and operational process design, including the first healthcare network fully compliant with Healthcare Information Exchange standards. Developed operational processes including assessment and mitigation strategies to optimize customer's Security Operations Centers. Defined security strategies to protect assets of a company responsible for more than a Trillion dollars. Defined the entire security architecture, operational plan, lights-out data center and SOC for one of the 5 largest US States. Defined and implemented security operations for US Government Agencies.

Previous Experience – *Senior Security Consultant, AT&T Security Consulting*
Beginning in 2006, led security consulting within AT&T and developed offers, trained consultants and let client engagements to achieve landmark and reference work, grow the practice and position new capabilities. Became the go-to person to resolve challenging issues and complex problems.

Previous Experience – *President and Principal Consultant, Gould Professional Services*
Incorporated in July 2001, served as President and Principal Consultant of the corporation. Performed security work for a broad spectrum of clients and security related tasks – clients included:

Blue Cross and Blue Shield
Roxanne Laboratories
Gardner Law Firm
City of Chesapeake
Cisco Systems
Quintiles Transnational
Able Information Security
Progress Energy
City of Virginia Beach
US Army
Novo Nordisk
SAIC / DIA
Port of Virginia
National Business Aviation Association
Boston Scientific

Tasks for these clients included Security Architecture Design, Perimeter Security Design, Security Policy Assessment, Security Policy Development, Firewall Installation & Rulebase Design, Teaching Firewall Engineering & Admin, Data Center Security Design, Intrusion Detection & Prevention Systems, Installation & Rule Base Development, Interior Enclave Security, Forensic Examination of Computers; Expert Witness Testimony (Computer Security Expert), Penetration Testing, Critical Infrastructure Security Assessment (physical, electronic and computer security), Regulatory Compliance Assessment (security) and Technical Compliance Remediation, Technical Surveillance Countermeasures, Database Security, Systems Security, Infrastructure and Architecture Security Evaluation and Remediation.

Previous Experience – *Product Manager, Optical and Broadband Services, Lucent Technologies*
2001-2003 Responsible for professional services management for 16 product lines from basic route and switch through complex multi-terabyte intercity trunking technologies. Defined operational strategy, policy, process and oversaw service delivery. Certified Product Manager.

Previous Experience – *Regional Security Resource Manager – International Network Services*
International Network Services, Inc. / Lucent Technologies: Responsible for the development, leadership and management of Mid-Atlantic regional Network Security consulting practice, including forensic and emergency response services. Defined and implemented services, training and staff development, sales and delivery processes. Developed Managed Security Services business. Consulted on startup strategy for Lucent's new ventures; responsible for B2B strategic relationship negotiations. Provided senior consultative leadership to client teams and executives.

Previous Experience – *Lead Security Manager, US EPA – Lockheed Martin Professional Services.*
Lead responsibility for Information Security at the US EPA's National Data Processing Center, including perimeter security, data integrity, systems and applications monitoring and management.

Previous Experience – *Vice President, Partner, Imagine Systems.*|
Information Security business targeting small to medium size IS customers. Marketing, technical sales, P&L responsibility. Developed one of the first real-estate search capabilities on the Internet in 1994, including all access, database, imaging and presentation technologies.

Previous Experience – *Producer and Recording Engineer, Bongiovi-Walters Productions, New York City.* Responsible for audio recording and production of special projects. Line producer for live TV broadcast, recording for syndication and live audience performance of The Early Days of Radio, a big-band entertainment season run with cast and crew of 60.

Previous Experience – *Senior Technical Associate, Bell Laboratories*
AT&T Bell Laboratories, Murray Hill, NJ. Laser Development, Computing Services (Murray Hill Computer Center), Computer Security (Bell Labs Computer Security Group), Lightwave Product Manufacturing, Visual Solutions (video teleconferencing); project manager, technical lead, responsible for engineering team; managed $M+ budget, Infosec Responsibility across 3 major data centers, 350+ systems from minis to Mainframes and Cray. Responsibilities also included semiconductor device physics, fiber and optical development engineering, test and measurement physics, VLSI Design and Test. Product Realization specialist including transfer to Manufacture. Quality Systems expertise. Solved major infrastructure problems with KDD/Japan's fiber backbone by identifying polarization dependence issues; Development team & test engineer, AT&T Advanced Video Processor (AVP) chipset (H.323 implementation, AVP4120, AVP4125), Advantest certified. Pioneer in Computer Forensics (first case 1986).

Key Areas of Expertise

Technology Skills

Data Networking

- Principal Security Architect for European Retailer w/900 outlets in 56 countries
- Special Security Implementations for classified networks/systems
- Principal Security Architect, State of Florida network
- Principal Security Architect, City and County of San Francisco
- Principal Security Consultant to $300M business that manages ~$1 Trillion in assets
- Network Forensics

Products

- Checkpoint Product Line
- Symantec Product Line
- Radware Product Line
- Cisco PIX, ASA, VPN concentrators; routers, switches, IDS
- Silent Runner
- Intellitactics SIEM, Q Radar SIEM, Fortigate Firewall, AT&T Aurora SIEM (Internal only, global scale)
- Encase, Access Data, Net Forensics Computer Forensics

Certifications and Training

- Certified Anti-Terrorism Specialist (CAS)
- Technical Surveillance Countermeasures certified Instructor (TSCM)
- Certified Information Systems Security Professional (CISSP)
- Checkpoint Certified Security Administrator / Engineer (CCSA/CCSE)
- Symantec Certified Product Engineer – Manhunt IDS (SCPE)
- Linux / Unix Systems Programmer / Developer (includes contributions to AT&T UNIX)
- FEMA Certified Emergency Manager
- NJ Certified Public Information Officer
- FCC General Radiotelephone License

Major Forensic Cases

- 1986 – Disclosure of National Security Information Discovered a leak of highly classified information and was able to identify the perpetrator within a group of 15 people. The FBI and US Naval Investigative Service brought this to resolution.
- Early 1990’s – US Secret Service investigation, “Mothers of Doom” hacker case At USSS Evidence Lab, in response to a request for assistance from USS SA Jack Lewis, performed evidence recovery and identified 800 pages of evidence, invalidating immunity of a suspect’s testimony in a proffer session.
- Late 1990’s – Interpath, a North Carolina Internet Service Provider (ISP) This ISP was a tier-1 (top level) provider infected with Stacheldraht malware. Investigated the live (running) server and identified that all evidence on disc had been deleted. The only remaining evidence was a running program in memory, which was recovered. This case changed the Best Practice in Forensics – no longer is the first step necessarily removing the power. Had that been done no evidence would remain in this case.
- Late 1990’s – As senior security administrator for the US EPA, investigated a complaint from the White House of computer intrusions and discovered an international attack involving 4 countries. Wrote monitoring and tracking software to capture the perpetrator online, brought together the FBI, Royal Canadian Mounted Police (RCMP), Scotland Yard and Deutche Bundespost in a live investigation tracking the intruder resulting in an arrest in Germany.
- South Carolina – A Public Works supervisor accused of violation of county policy was fired and brought countersuit. Forensic investigation recovered 4 3” thick binders of evidence showing sexual misconduct. Countersuit dismissed.
- Discovered Al Qaida attack plans targeting US Soil. Working with the FBI, the perpetrator, who was a foreign citizen in the US. Arrest made within 48 hours and the attack was thwarted.
- Mid-2000’s – Florida vs. Rabinowicz – in a case where possession of contraband was the only element of proof, stipulated that the contraband was authentic and present. I proved forensically that the defendant was not technically in possession of the evidence and that evidence was planted. Qualified as an expert witness and provided expert testimony in this case.
- Mid-2000’s – Identified a leak of national security from Oak Ridge National Laboratory involving chemical weapon information using forensic analysis and was able to identify the perpetrator. DSS responded and resolved the case.
- Mid-2000’s – Investigated sabotage of a health industry contractor. The systems administrator had been fired and sabotaged the system. Solved the case and the administrator went to prison.

Instructor of Forensics

- Taught Forensics and Advance Forensic Techniques to State Law Enforcement, Military and major corporate customers at the World Institute for Security Enhancement.

- Taught Technical Surveillance Countermeasures (TSCM) course for government and industry at the World Institute for Security Enhancement.
- Wrote the entire course and taught the entire CISSP curriculum at Able Information Systems.