Committee on Energy and Commerce
U.S. House of Representatives

Witness Disclosure Requirement - "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

1. Your Name: Dale Drew		
2. Your Title: Senior Vice President, Chief Security Officer		
3. The Entity(ies) You are Representing: Level 3 Communications		
4. Are you testifying on behalf of the Federal, or a State or local government entity?	**Yes**	**No** X
5. Please list any Federal grants or contracts, or contracts or payments originating with a foreign government, that you or the entity(ies) you represent have received on or after January 1, 2013. Only grants, contracts, or payments related to the subject matter of the hearing must be listed.		
6. Please attach your curriculum vitae to your completed disclosure form.		

Signature: [redacted] **Date: 11/14/2016**

Dale Drew

Who Am I

I am a technologist; I am a Security Architect. A global leader who builds high performing teams that solve some of the industries largest and most complex security issues. I manage global certification and regulatory environments that govern communications services, applications, data privacy and ethics.

Experience

Dale Drew is an accomplished and experienced corporate security executive with 29 years of experience in developing critical global security programs, working in Federal/State Law Enforcement and with Internet Service Providers (ISP).

Dale brings a practical capability to integrating security into the culture of the business, enabling the company to be more flexible, with demonstrable results. He is an experienced leader in creating high performance teams, designing innovative security solutions, handling global regulatory environments, managing highly technical personnel, and resolving conflict.

Dale is currently the Chief Security Officer at Level 3 Communications, a global telecommunications service provider specializing in Optical, Internet, VoIP and CDN services. At Level 3 Communications, Dale directs all aspects of Security; Security Policy, Physical and Logical Security, Federal Programs, Governance , Corporate Investigations and Managed Security Services. Dale manages global Architecture, Engineering, Operations and Compliance teams.

Dale has designed, built and deployed internal and commercial-grade security infrastructure and threat analysis systems used to monitor and protect some of the most sophisticated and largest global networks. He has extensive computer forensic capabilities.

Prior to Level 3 Communications, Dale worked for Qwest Communications and MCI, where he was responsible for Internet Security Operations and Engineering. Dale has also worked for the U.S. Secret Service where he spearheaded Operation Sundevil, the nation's largest computer crime investigation. Dale also ran the Arizona state forensic lab, working for the Attorney General's Office in the Organized Crime Division.

Apr 1999–Present Level(3) Communications Broomfield, CO

Chief Security Officer / Vice President, Global Security

- Am responsible running Level 3's Global Security program, which consists of: Physical Security, Logical Security, Business Continuity, Investigations, Managed Security and Government Programs (FISMA, DCID, and PSN

CAS(T) environments). Maintain Architecture, Engineering, Operations and Program Management functions.

- Responsible for global security policy, regulatory compliance to keep Level 3 in compliance with data security, privacy and regulatory compliance.
- Operate Level 3's Policy program which is compliant with ISO 27001:2005 and NIST 800-53v4 (Moderate), including the global Education and Awareness programs and policy effectiveness and compliance programs on a global level in LATAM. EMEA and the US.
- Run Level 3's Managed Security Services which includes a globally deployed Managed Services capability to its customers that offer UTM, Anti-Virus, NIDS, NIPS, Anti-Spam, an internally developed DDoS detection and Mitigation infrastructure, an internally developed Threat Intelligence and Situational Awareness infrastructure, Secure Remote VPN Access, and a Managed Security Operations Center product. This responsibility includes Architecture, Engineering and global Security Operations Centers capability.
- Run the Level 3 Global Security Compliance organization that organizes certification frameworks, internal and external Red Team/Penetration testing, and policy framework and compliance verification. Certification framework consists of; FISMA, DCID, NISPOM, SSAE16, PSN CAS(T), UK IL2, US IL3, PCI DSS, SOX, HIPAA, and ISO27001:2005.
- Maintain responsibility for reviewing global cybersecurity related legislation and providing the company a focal point for response, coordination and impact analysis.
- Responsible for maintaining the company's quarterly, yearly, and three year Security Strategic Roadmap and aligning that roadmap across all appropriate stakeholders in the company for agreement and resources to ensure success of the Global Security program.
- Was responsible for developing the business case that restructured Level 3's distributed Security Organization structure into a centralized, holistic security organization.
- Coordinate and report to the Board of Directors Audit Committee and Security Committee.
- Responsible for ensuring a safe and complete security integration of all company acquisitions performed by Level 3. This involves integration of companies that were just as large as Level 3 and ensuring the business still has the capability to remain flexible and adaptable and quick to market, while ensuring a risks were quickly evaluated, mitigated and corrected.
- Designed and implemented infrastructure that would automatically inventory production applications, register the application and systems owner and perform an automated initial security risk assessment for SoX, HIPPA, GLBA, FISMA and security policy compliance.
- Designed and implemented a carrier grade Distributed Denial of Service detection and mitigation infrastructure for the Level 3 backbone network.
- Responsible for ensuring the security and fraud counter measures for Level(3)'s Voice Over IP SIP services; including the design of the industry's first commercial statefull SIP firewall.
- Deployed an intelligence collection infrastructure that automatically collected, analyzed and categorized network and application threats that were then analyzed in Security Architecture's prototype lab.

Sep 1998–Apr 1999 Qwest Communications Reston, VA

Director, Network Security

- Managed Qwest's Security Architecture, Engineering and Operations departments: responsible for protecting Qwest's global revenue products, services and management networks. Built organizations from the ground up.
- Designed Qwest's security infrastructure; responsible for monitoring and proactively ensuring the security of Qwest's core, edge and service networks.
- Responsible for designing and developing Qwest's commercial security product offerings. Products included: Managed Firewall (CPE) (Checkpoint/Cosine based), Exposure Analysis Scanning, and Security consulting. Developed Value Proposition and Business Case.

Jul 1991-Sep 1998 MCI Telecommunications Reston, VA

Manager, Security Engineering

- Responsible for Security Engineering and Security Architecture of MCI's global data networks, including: Frame Relay, internetMCI, and Tymnet (X.25).
- Designed MCI's data security infrastructure; responsible for monitoring and proactively ensuring the security of MCI's production networks.
- Responsible for designing and developing MCI's world class security product offerings. Products included: Managed Firewall (CPE); a Checkpoint based managed firewall service that included intrusion detection, dial and network VPNs, consulting, and the industry's first web-based exposure analysis system.
- Deployed an intelligence collection infrastructure that automatically collected, analyzed and categorized network and application threats that were then analyzed in the security lab.
- Brought organization into ISO-9001 compliance.

Jul 1988-Jul 1991 AZ Attorney Generals Office Phoenix, AZ

Evidence Analyst

- Responsible for Arizona's first formalized computer crime lab center, analyzing computer related criminal evidence. Cases ranged from computer hacking, child pornography, telemarketing, burglary and drug enforcement.
- Provided court testimony relating to investigative procedures and evidence analysis for specific cases.

Aug 1987-Jun 1991 US Secret Service Phoenix, AZ

Analyst

- Provided investigative services for nation's first, and at the time, largest nation-wide computer crime sting operation yielding searches in 23 homes in 17 states.

Media

Featured in major national publications for my work relating to Cybersecurity research and Internet related threats.

Blogs: http://blog.level3.com/author/dale-drew/

- Ransomware: A Real Horror Story
- Anatomy of a Nation State Hack
- How Advanced Persistent Threats Happen
- Cybersecurity: Get it done

YouTube:

- Internet Safety Month Week 4: What is the Threat Landscape with Dale Drew
  - https://www.youtube.com/watch?v=2C7WFsnxYR8
- How Do You Secure Your Connected Home?
  - https://www.youtube.com/watch?v=udPNjvDiyrQ
- BASHLITE Malware | Between Two Threats
  - https://www.youtube.com/watch?v=Mmv2mxUTx4I
- Shadow Brokers | Between two Threats
  - https://www.youtube.com/watch?v=dOxq2Pgi1mg
- Industry Collaboration is Key to Security
  - https://www.youtube.com/watch?v=qjCoXkNZhDU
- Inside an Internet of Things House
  - https://www.youtube.com/watch?v=h4M3yz5WIlY
- The Level 3 Security Solution Difference
  - https://www.youtube.com/watch?v=fyRAV7ckHzU

Media:

- How one rent-a-botnet army of cameras, DVRs caused Internet chaos
  - http://arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet/
- **Musicians May Be The Key To The Cybersecurity Talent Shortage**
  - http://www.content-loop.com/musicians-may-be-the-key-to-the-cybersecurity-talent-shortage/
- US takes aim at cyberattacks from connected devices as recalls mount
  - http://www.cnbc.com/2016/10/25/us-takes-aim-at-cyberattacks-from-connected-devices-as-recalls-mount.html
-
- Level 3 Tries to Waylay Hackers
  - http://www.wsj.com/articles/level-3-tries-to-waylay-hackers-1432891803
- Hackers Infect Army of Cameras, DVRs for Massive Internet Attacks
  - http://www.wsj.com/articles/hackers-infect-army-of-cameras-dvrs-for-massive-internet-attacks-1475179428