II.E.4 Key Personnel

Key Technical Staff **(% Time on Project)** **Proposed Role on Project**	**Experience**

Greg Hoglund (15%)
Principal Investigator
	Chief Executive Officer, HBGary Inc. Sacramento, CA (Dates)
	• Chief architect of commercial cyber security software products:
	  ○ Digital DNA, Responder and Recon
	• Created and documented first Windows kernel rootkit
	• Pioneered new technologies to automatically reverse engineer software binaries from within computer memory
	• Developed technologies to automatically harvest malware behaviors during execution.
	• Published numerous significant works in cyber security field, including:
	  ○ *Rootkits: Subverting the Windows Kernel; Exploiting Software: How to Break Code; An Exercise in Advanced Rootkit Design; Runtime Decompilation; Exploiting Parsing Vulnerabilities; Kernel Mode Rootkits; A *REAL* NT Rootkit, Patching the NT Kernel.*
	Founder and CTO of Cenzic (Dates)
	• Developed Hailstorm, a software fault injection test tool

Aaron Barr (15%) Program Manager	**President, HBGary Federal LLC Sacramento, CA** (Dates) • Developer and integrator of cyber security software products for the Government and IC **CTO, Northrop Grumman,Cyber and SIGINT Systems Business Unit** (Dates) • Developed and implemented technical strategy and ensuring quality technical execution across $700M organization • Managed a $20M R&D program across Cyber, SIGINT, Airborne, and Special Access Programs **Chief Engineer, Northrop Grumman, Cyber Security Integration Group** (Dates) • Developed and planned corporate cyber security strategy
Jason Upchurch (25%) Senior Technical Lead for Intrusions Forensics	**Senior Technical Lead, GDAIS Cyber Systems, Centennial, CO** (Dates) • Leads incident response and forensics on computer intrusions for Director of Cyber Systems • Technical manager and subject matter expert in malware analysis and intrusion forensics o Provides mentoring/coaching to other cyber systems personnel o Develops automation techniques for digital forensics o Provides internal and external training on Malware Analysis and Large Dataset Forensics **Technical Lead, DoD Computer Forensics Laboratory (DCFL) Intrusion Section**(Dates) • Led malware analysis development at DoD Cyber Crime Center as Center's first malware analyst • Instrumental in guiding the process for malware analysis and cyber intelligence within DoD **Contract Manager, National Cyber Investigative Joint Task Force (NCIJTF)** (Dates) **Contract Manager, DoD Collaborative Investigative Environment (DCISE)** (Dates)
Tom O'Conner (100%) Research Lead	**Senior Technical Lead, Pikewerks, Alexandria, VA** (Dates) • Supports development of government and commercial software security products • Develops Windows and Linux security products in multiple languages and relational databases: o C, C++, Java, and Python o Microsoft SQLServer, MySQL, and IBM DB2. **Research Lead, Cyveillance, Location** (Dates) • Internet researcher for compromised data and malware sites and IRC Channels. • Operated monthly web crawl and index of over 100 million domains, o Increased automation and predictability. **Research Lead, Cigital, Location** (Dates) • Developed source-based software security tools for both C and Java o Research into fault injection to identify software security flaws presented at 1998 IEEE Symposium on Security & Privacy • Supported Java Security; co-authored appendix on Java code signing in "Security Java" book
Kenneth Prole (25%) Research Lead	**Project Engineer, Applied Visions, Inc., Secure Decisions Division**, **Northport, NY** (Dates) • Develops visualization solutions for both government and commercial clients • Leading DARPA funded wireless transmitter visualization SBIR project called MeerCAT • Leading visualization development for DARPA sponsored National Cyber Range program • Led security visualization in large scale government research projects for DARPA and DHS • Patent Pending for Multilayer Wireless Network Flow Graph • TS Clearance • Coauthored selected Publications include o "Advances in Topological Vulnerability Analysis," in *Proceedings of the Cybersecurity Applications & Technology Conference for Homeland Security 2009*; "Wireless Cyber Assets Discovery Visualization," in *VizSec 2008;* "A Graph-Theoretic Visualization Approach to Network Risk Analysis," *VizSec 2008*

Phillip Porras (25%)
Research Lead
	Program Director, SRI International, Computer Science Lab, Menlo Park, CA (Dates)
	• Principal Investigator in a multi-organization NSF research project: "Logic and Data Flow Extraction for Live and Informed Malware Execution."
	• Lead research into malware pandemics on next generation networks for Office of Naval Research
	• Principal Investigator of a large ARO-sponsored research program entitled Cyber-TA
	  ○ Developing new techniques to gather and analyze large-scale malware threat intelligence
	• Developed prototype technologies including:
	  ○ BotHunter, BLADE, Highly Predictive Blacklists, and Eureka malware unpacking system
	  ○ Holds eight US Patents
	Program Manager, Aerospace Corp., Trusted Computer Systems Department, Location (Dates)
	• Experienced trusted product evaluator for NSA
	  ○ Performed security testing, risk assessment, and penetration testing of systems and networks
	• Awarded Best Paper honors in 1995, 1999, and 2008

Dr Dawn Song (20%) Researcher	**Associate Professor, UC Berkeley, Berkeley, CA, 2007-Present** • Lead Project BitBlaze, binary analysis for security applications, awarded MIT Technology Review TR-35 • Ph.D. Computer Science • Multiple Awards in computer security research **Assistant Professor, Carnegie Mellon University, Pittsburgh, PA, 2002-2007**
Dr Anita D'Amico (25%) Researcher	**Human Factors Researcher, Applied Visions, Inc., Secure Decisions Division, Northport, NY**(Dates) • Human factors psychologist and a specialist in information security situational awareness • Ph.D. Psychology, Adelphi University • Researcher into visualization cognitive analysis, operational fatigue, and research methods
Andrew Tappert (100%) Researcher	**Technical Researcher, Pikewerks, Alexandria, VA** (Dates) • Refine function extraction methods and develop automation of methodologies • Nine years experience with rootkits, malware, and other kernel/low-level software development • Developed software for CIA Information Operations Center • M.S. Computer Science, Stanford University