**TODD FINKLER**

NCUA Senior Executive, Active TS/SCI

(443) 302-9345 [todd.finkler@gmail.com](mailto:todd.finkler@gmail.com) [www.linkedin.com/in/todd-finkler](http://www.linkedin.com/in/todd-finkler)

**Experience Summary**

35+ years of experience leading people, exploring innovative solutions, and developing and integrating technology to solve complex challenges as both a Senior Leader and Military Officer. Partnered with and served multiple Executive branch agencies, Legislative branch, numerous international standards organizations, and several U.S. and international research organizations. Applied data to solve hard problems in information technology and cybersecurity on topics such as cloud and zero trust architectures, 5G mobile network and wireless security, Internet of Things security, wireless routing algorithms, validations of cryptographic implementations, automated vulnerability analysis, securing AI/ML, supply chain risk management, and hardware security mechanisms using machine learning and automated techniques.

**Skills Summary**

Influential Leader

* 35+ years of leadership experience as a Senior Executive and Military Officer of teams of 100+.
* Clearly defined vision and established innovative culture in three large organizations.
* Outstanding servant leader that empowers entire workforce to own the mission.

Innovative and Critical Thinker

* Embedded lean lifecycle into organization culture, ensuring rapid, dynamic ideas-to-application.
* Strong reasoning, problem solving, and ideation skills proven applied to diverse technology challenges: Cybersecurity, Cloud Computing, Wireless Communications, and Information Technology.

Change Agent

* Aligned strategic plans by setting clear objectives and key results to track performance of tens of $M+ efforts.
* Engaged executive management to establish critical priorities, defined success criteria, and set clear direction for the team.

**Education**

**Master of Science in Electrical and Computer Engineering** - Univ of Maryland College Park

**Master of Business Administration, Information Systems** - Univ of Maryland College Park

**Bachelor of Science, Aerospace Engineering with Merit** - United States Naval Academy

**Continued Learning Courses:**

* Supervised Machine Learning – Standford
* Data Science Fundamentals – Johns Hopkins
* Practical Machine Learning – Johns Hopkins
* Python for Data Science, AI & Development – IBM
* Mathematics for Machine Learning: Multivariate Calculus – Imperial College of London
* Google Cloud Big Data and Machine Learning Fundamentals – Google Cloud
* Modernizing Data Lakes and Data Warehouses with Google Cloud - Google Cloud
* Artificial Intelligence A-Z 2025: Agentic AI, Gen AI, and RL - Udemy

**Professional Experience**

2022 – Present **National Credit Union Administration (NCUA)**

**Chief Information Security Officer**  Mar 2024 – Feb 2025

Senior Executive, 50 hours/week

Drove strategy, advised the NCUA Board and the Executive Director on enterprise risk to the information technology infrastructure that enables the NCUA mission.

Key Duties:

* Lead People/Manage Resources – Lead the NCUA cybersecurity team to reduce cybersecurity risk for the NCUA through cybersecurity technology integration and application and improving cybersecurity operations.
* Lead Change/Achieve Results – Improve risk mitigation performance for the NCUA information technology system through integration of security technology and development of robust security processes. Drive change towards quantified cybersecurity risk measurement.
* Build Coalitions/Communicate – Advised the NCUA Board and the Executive Director on cybersecurity risks internal to NCUA. Connect with the cybersecurity community to share threat information and collaborate on incidents.

Selected Accomplishments:

* Lead People/Build Coalitions/Communicate/Achieve Results: Improved DevSecOps processes to focus energies on highest risk reduction activities. For example, examined the existing vulnerability management process, recognized confusion of responsibility, established zero-deviation/policy-focused goals, drove data visualization to communicate outstanding vulnerabilities from the security team to the three operational teams, established weekly status checks, briefed performance updates to senior leaders, and prioritized remaining vulnerabilities to minimize risk. Ultimately, the increased attention reduced outstanding vulnerabilities 40X with a trajectory towards zero deviations in 3 months.
* Leading Change/Achieve Results: Changed decision-making/prioritization to focus on highest risk reduction activities to manage the deluge of operational requirements. Adopted improved project management techniques/tools and shifted work from individual contributions to project-based outcomes based on Agile techniques. Examined and changed data extraction to ensure details available for resulting quantified risk analysis. Worked to understand and remove roadblocks. These efforts reduced stress and increased the impact of the team, prioritized the efforts towards solving key challenges, and aligned energies towards the NCUA strategic objectives.
* Manage Resources/Communication: Recognized the excessive load of activities from prior year budgets which constrained the ability to mature the newly installed security tools. For the 2025 budget requests, reviewed all cybersecurity team requests, drove a prioritization based on both the team’s strategy for 2025 and tool-based risk reductions, reduced the requested items to ensure strategic objectives were met, developed justifications for the remaining items, and reviewed/edited presentations for ITOC’s budget reviews. These efforts resulted in clear and effective budget request documentation with several senior leaders commenting on clear presentations.

**Cybersecurity Executive**  Nov 2022 – Present

Senior Executive, 50 hours/week

Drove strategy and advised the NCUA Board and the Executive Director on cybersecurity and financial sector critical infrastructure matters internal to NCUA and across the nearly 5000 US credit unions.

Key Duties:

* Lead People/Manage Resources – Lead cybersecurity thinking for the internal enterprise information technology and the 4000+ credit union sector.
* Lead Change/Achieve Results – Drive financial sector critical infrastructure cybersecurity strategy across the 4000+ US credit unions. Initiate cybersecurity risk measures towards quantitative decision-making.
* Build Coalitions/Communicate – Advised the NCUA Board and the Executive Director on cybersecurity and financial sector critical infrastructure matters internal to NCUA and across the nearly 4000+ credit unions. Connect with the cybersecurity community to share threat information and collaborate on incidents.

Selected Accomplishments:

* Lead People/Communications/Build Coalitions: Ensured the NCUA acted as one to mitigate systemic credit union risks during major credit union cybersecurity outage. Translated technical information for the NCUA Board of Directors/US Treasury, reviewed/edited/approved multiple press releases, fostered regional communication with affected credit unions, and shared information across the NCUA. Prepped the NCUA Chairman for financial sector discussions. Coordinated information/wrote messages to Congress. Connected with commercial vendor senior leadership to share information. Drove after-action improvements across 6 directorates and US Treasury.
* Build Coalitions/Achieve Results/Communication/Lead Change/Lead People: Examined the cybersecurity risk to the NCUA mission posed by the credit unions. Researched 16 papers on cybersecurity risk affecting the banking sector, connected with experts in the Federal Deposit Insurance Corporation/Federal Reserve Board/Financial and Banking Information and Infrastructure Committee/Treasury, attended the MIT/FRS Conference on Measuring Cyber Risk in the Financial Services Sector, learned about the operation of the NCUA’s share insurance fund, wrote a summary paper on systemic cyber risk that threatens the NCUA’s share insurance fund, gained feedback from regional information security officers and experts across the NCUA, and developed a systemic/non-systemic risk presentation for the senior leaders of the Enterprise Risk Management Council (ERMC). Innovative thinking on systemic risk delineated current exposures, existing challenges, and next-step responses. Sparked change to prioritization process from number-of-credit-unions to an asset-impact model to more accurately align resources towards the highest systemic cyber risks.
* Manage Resources/Communication: Managed external and internal cybersecurity risk for the NCUA. Applied cybersecurity expertise through analysis of strategies, communications, audits and operations of multiple offices across the NCUA and credit unions to anticipate problems and identify solutions that mitigate cybersecurity risk to match the NCUA’s low risk appetite. In addition to the improved coordination and communication of cyber incidents, evidence of mitigations include: recognized the weakness in vulnerability management and cloud architecture security and successfully advocated for additional resources; examined compliance activities and highlighted challenges in program management; recognized credit unions’ cybersecurity resource constraints, found free resources offered by federal institutions, and communicated those resources to increase the connections; observed a breakdown in communication of an external web attack with the NCUA’s primary resources and used that example to develop internal incident response playbook for improved future communications; and reviewed hundreds of reports/threat information/press releases on cyber threats and ensured appropriate offices received the reports for action.
* Lead Change/Lead People: Agent of change for credit unions cybersecurity incident reporting. Integral part of the implementation of the NCUA’s Cyber Incident Rule Reporting. Reviewed, edited, and commented on the draft rule. Addressed rule questions from Vice Chairman and Deputy Executive Director. Reviewed and edited requirements for the Cyber Incident Reporting Tool and accelerated when stalled and behind schedule. Drove tool development through weekly status meetings over 5 months to be prepared for the rule activation. Explored the data security of captured data in the system, balancing useability of the tool, security of the data, and automation of the reporting mechanism. Edited the messaging to the credit unions about the reporting requirements and start date. Tool successfully supported reporting by rule activation.
* Lead Change/Communication: Created a vision for maturation of the NCUA’s internal cybersecurity capabilities. Reviewed six information security assessments that occurred in the last three years. Wrote a summary of the assessments, grouping the findings for analysis and decision-making. Prioritized and recommended a way forward to address the open findings. Collaborated with the Chief Information Officer to gain buy-in for the strategic direction/recommendations. Strategy presented to the NCUA Board to support additional personnel resources to strengthen vulnerability management, develop cloud architecture, and create a cloud cybersecurity strategy.
* Lead Change/Manage Resources/Build Coalitions: Championed Executive Order on Improving the Nation's Cybersecurity (EO14028) efforts. Recognized White House frustration with slow compliance. Analyzed EO14028 and examined NCUA’s compliance status. Analyzed the National Institute of Science and Technology’s Zero Trust Architecture and draft Implementation documents to understand the maturity of the requirements. Defined basic compliance requirements and engaged the Chief Information Officer team for technical details of status on each item to determine what items are still deficient. Initiated senior executive report on status. Extensively edited report and brief in preparation for a meeting with the NCUA Board Chairman on Cybersecurity work progress. Initiated development of a strategy to align with the overall information operations strategy.
* Build Coalitions/Communications: Established a strong connection with Cybersecurity and Infrastructure Security Agency (CISA) to amplify their support to credit unions with cybersecurity expertise and services. Discovered a series of services that CISA provides critical infrastructure entities and communicated that to credit unions. Connected with the Vulnerability Management Products and Services, High Value Asset, Stakeholder Engagement, Vulnerability Discovery, and National Risk Management teams to communicate services to credit unions. After passage of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022, reviewed CISA’s CIRCIA reporting rule and connected with their legal and project management teams to work towards single reporting. Worked with CISA to provide a live webinar to credit unions on protecting individual credit and identity through cybersecurity awareness, developing slides and covering for a CISA member during last-minute cancelation. Moreover, reviewed and provided feedback on Financial Sector Cyber Performance Goals to help credit unions prioritize their cybersecurity efforts. Additionally, connected with CISA’s Joint Cyber Defense Collaborative to gather/analyze/share actionable cyber risk information to enable synchronized cybersecurity planning/defense/response.
* Build Coalitions/Communication: To ensure the NCUA Board could effectively build coalitions, supported the NCUA Board Chairman for Senate and House hearing, Government Affairs Conference 2024 cybersecurity discussion by meeting with President and CEO of National Association of State Credit Unions Supervisors, authoring general NCUA cybersecurity summaries, communicated the challenges of not having third-party authority, regular meetings with Vice Chair Policy Advisor, and reviewed/edited multiple sections of the CY2024 Annual Cybersecurity Congressional Report.
* Build Coalitions/Communication: Drives national and the NCUA strategy through leadership in external (e.g. Financial and Banking Information Infrastructure Committee, Cyber Incident Reporting Council, Cyber Forum for Independent and Executive Regulators, Federal Financial Institutions Examination Council, and Financial Services Sector Coordinating Council) and internal councils (e.g. Cybersecurity Council, Information Technology Operations Council, Enterprise Risk Management Council, Technology Advisory Committee, Digital Asset Working Group, and Fintech and Access Steering Committee). Drove discussions by presenting regularly, reported to the NCUA Board Chairman on meeting results, analyzed and offered recommendations for several challenges delineated during council discussions, analyzed budget recommendations, planned and coordinated of meeting agendas, reviewed and edited meeting minutes.
* Lead Change/Build Coalitions/Communication: Identified and reduced the NCUA cybersecurity incident risks. Cyber incidents from external and internal sources were not consistently nor systematically communicated outside of siloed offices, causing missed opportunities to prepare for and appropriately manage each incident. Pulled together a cross-NCUA team and examined recent incidents for gap analysis. Defined accountable organizations for internal and external cyber incidents. Wrote NCUA Cyber Incident Coordination Playbook that outlined organizational responsibilities for each cyber incident. Defined common severity level for internal and external incidents and defined communication at each level. Streamlined communication on and created knowledge base for future incidents. Developed an automated Day-1 reporting mechanism that clearly answered standard questions for senior leadership, dramatically increasing the speed of communications from weeks to hours. Broke down silos across multiple NCUA offices and improved cybersecurity contract language on managed contracts. Reviewed, commented, and edited six cybersecurity threat messages to credit unions and coordinated their approval through the NCUA Executive Director.
* Build Coalitions/Communications: In preparation for the upcoming Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) regulations being established in early 2025, Todd drove the development of a web form for the NCUA’s current cyber incident reporting rule to ensure that the CIRCIA requirements could be met by automating the forwarding of credit union web submissions received by the NCUA onto the CISA incident reporting system to prevent dual reporting requirements. Reviewed requirements for web form, pushed to get appropriate funding to cover the effort, coordinated requirements with CISA’s CIRCIA draft rule, drove needed automation and development of web form to expand ease of reporting and processing reports, ensured necessary cyber incident data is reported, and prepare for future mandatory reporting to the CISA. His work ensured the web form was completed and prepared to perform the automation step when CISA finalizes it cyber incident reporting collection system.

2002 - 2022 **National Security Agency (NSA)**

**NSA Chief Data Scientist and Senior Data Science Authority** Sep 2021 – Oct 2022

Defense Intelligence Senior Leader, 50 hours/week

Cultivated a sustainable Agency Data Science ecosystem through coordinating data science investments, improving data science readiness, and measuring data science impact across the Agency.

Key Duties:

* Lead People/Manage Resources – recruit, develop, and retain ~1100+ data science employees across NSA. Ensure resources are available to meet strategic growth of data science.
* Lead Change/Achieve Results – Define strategic plan to hire, develop, and retain data science expertise and improve readiness to meet Agency needs. Assess data science health details across the Agency through customer focus efforts and work towards solving problems to increase technical health.
* Build Coalitions/Communicate – Build connections to senior leadership across all NSA missions to understand and meet data science and artificial intelligence/machine learning (AI/ML) needs.

Selected Accomplishments:

* Lead People/Lead Change/Manage Resources/Build Coalitions: Established a collaborative, cross-mission working environment to recruit, develop, and retain ~1100+ data scientists to meet the data science and artificial intelligence/machine learning needs. Clarified gaps, developed strategy, and defined a data-driven plan of action to increase both the number and quality of data science hires. Communicated the need for significant resource plus-up through frequent oral and written presentations and papers, influencing a 10X increase in budget from thousands to multimillions of dollars.
* Lead Change/Manage Resources: Explored and evaluated opportunities to integrate emerging technologies to assess individual skills to provide more accurate, data-supported supply of data science core competencies to drive hiring, internal skills development, diversity, and retention.

**Applied Cybersecurity Research Chief, NSA** Nov 2019 – Aug 2021

Defense Intelligence Senior Leader, 50 hours/week

Established CFS organization from the ground up to dynamically de-risk emerging cybersecurity solutions that achieve asymmetric advantage over cyber adversaries in partnership with Industry and Academia.

Key Duties:

* Build Coalitions – Build external trusting partnerships and encouraged connections to mission customers to support Cybersecurity strategic plan. Facilitate prioritization of standards efforts relating to mobile and enterprise security across 11 national and international security standards development organizations (e.g. National Institute of Standards and Technology, 3rd Generation Partnership Project Mobile Networks, The Institute of Electrical and Electronics Engineers, etc.) within the confines of existing resources and pushed for additional resources to increase cybersecurity impact.
* Establish a Cybersecurity Standards Center - Guide instantiation and development of the NSA's Center for Cybersecurity Standards (CCSS) by strengthening partnerships with NSA mission customers, research, external standards organizations and defining roles and responsibilities.
* Lead Change - Create an innovative, agile environment using design thinking to systematically generate ideas, explore assumptions relevant to mission adoption, jointly validate specific solutions, learn from failures, and manage risks that securely use, processing, storage, and transmission of information or data with operationally focused organizations.
* Drive Results – Work using advanced technology and innovations development and deployment process to ensure rapid and dynamic ideas-to-application through validating assumptions and mitigating risks from the start, looking to build the next most valuable cybersecurity solution the simplest way and as fast as possible. Drive successful solutions towards operational development and deployment.
* Lead People - Manage the hiring process to include development of position descriptions, performance profiles, and interview guides. Personally, interview all candidates to ensure the right candidates were selected for critical leadership roles. Develop training opportunities to build creative people, innovative teams, and mission outcomes. Encourage taking risks and learning from failure. Facilitate identification of skills gaps and developed a strategy to close the gaps.
* Business Acumen - Establish budget baseline through alignment with strategic objectives. Ensure obligation and execution budget. Prioritize and execute explorations and insertions of new cybersecurity technology into the mission space considering budget guidelines and constraints.
* Build an Organization - Lead a diverse executive staff and cybersecurity experts to build organizational structure, communicate a vision, create innovative environment, and create internal controls to manage risk.

Selected Accomplishments:

* Lead Change/Achieve Results/Build Coalitions: Established the organization through close executive management collaboration, increasing the multimillion-dollar budget ~4X in a year and more than doubled the size of the organization in 3 months to exceed 50 on growth towards 100+.
* Lead People: Created innovative culture of asking questions, defining assumptions, listening carefully, and proving validity which empowered innovation inspired team members to take ownership of mission outcome - all vital to survive the complex threats in a dynamic cyber threat environment!
* Achieve Results: Initiated and prioritized 20+ technology explorations into advanced technologies including cloud security, zero trust, network/software security analysis, securing Al/ML, and 5G mobile network security that focused on application of detailed security principles towards secure use, processing, storage, and transmission of information or data. Based on agile development processes, defined clear goals and measurable outcomes to allow team members to take ownership of creative and diverse solutions and integrate solutions with mission customers.
* Lead Change: Overcame COVID restrictions preventing work from traditional locations to maximize mission impact. Experimented with and adopted alternate virtual work tools and techniques, sought necessary equipment for all employees to succeed working virtually, and redesigned group workflow to maximize mission success in the virtual environment. These efforts guided an NSA-wide effort to rethink teleworking, ensured continuity of the standards mission, and enabled COVID high risk individuals were still able to support missions.

**Cybersecurity Research Technical Director, NSA** Aug 2016 - Aug 2019

Defense Intelligence Senior Leader, 50 hours/week

Develop, coach, and guide researchers to develop core research strategies and communication tools towards increased collaboration and development and deployment of advanced, modern technologies into multi-faceted mission environments.

Key Duties:

* Lead People – Lead researchers. Develop training opportunities to build creative people, innovative teams, and mission outcomes. Encourage taking risks and learning from failure. Facilitate identification of skills gaps and developed a strategy to close the gaps. Developed leaders through individual mentoring and weekly leadership discussions, covering topics on Leadership, Innovation, Motivation, Human Behavior, Diversity, Decision-Making, and Technology.
* Lead Change - Create an innovative environment and new work process to generate ideas, explore assumptions relevant to mission adoption, jointly validate specific solutions, mitigate risk, loop back learning from failures, adapt to rapidly changing environments, and deploy into mission jointly with operationally focused organizations. Create and embed a research proposal methodology that aligned research efforts towards defined objectives and key results and improved the individual researcher's ability to transfer research.
* Drive Results – Initiate advanced and modern research on Security and Risk Mitigation using design thinking to systematically decide on successful solutions through exploration of numerous new research directions to include distributed and private machine learning data networks, data science anomaly detection applied to cyber defense, increasing usability of deep technical security capabilities, risk reduction of virtualization and physical separation, and on body communication. Integrate successful technologies into operational information technology environments.
* Build Coalitions - Define objectives and guide outcomes towards mission value as a board member for research senior leaders across the department of defense (Cyber Community of Interest, Joint Artificial Intelligence Center project reviews), three federally funded research organizations, innovation counsel, multiple international research organizations (The Technical Collaboration Partnership among others), and cross-federal government wireless steering group.
* Customer Service – Create research transfer opportunities of modern, advanced security solutions to security engineering customers including automated vulnerability discovery, finding unintended transmissions using software defined radios, fused data for machine learning, monitoring of software defined networking, deception to increase security, hypervisor integrity monitoring, and applying general artificial intelligence to cybersecurity.
* Business Acumen - Prioritize and execute research efforts considering alignment with strategic objectives and budget guidelines and constraints.

Selected Accomplishments:

* Fostered partnerships with a diverse set of senior leaders of multiple mission organizations and used agile processes to integrate research into operational information technology systems to mitigate cybersecurity risks for technologies such as wearable authentication, validation of cryptographic implementations, secure mobile platforms, integrity monitoring, supply chain risk management, and secure enclaves to increase the secure use, processing, storage, and transmission of information or data or to mitigate security risks.
* Worked with the U.S. Senate Select Committee on Intelligence to answer technical questions on hypervisor security, wrote a virtualization strategy to meet the needs of congressional inquiry, and responded to congressionally directed action which ultimately supported additional funding.
* Collaborated to determine relevance of unintended emanation threat to existing wireless environment and advanced an initial research proposal to define criteria that would minimize wireless risk and presented findings to the Deputy National Manager for National Security Systems.

**Cybersecurity Engineering Group Technical Director, NSA** Jun 2013 - Jul 2016

Defense Intelligence Senior Leader, 50 hours/week

Develop cybersecurity expertise and create standard secure architectures for building and operation of national security systems.

Key Duties:

* Lead People - Develop cybersecurity engineers to methodically understand system risk and apply appropriate mitigations.
* Develop and Publish Secure Architectures and Mitigate Risks – Create secure architecture guidance to build and approve secure wired and wireless networks using modern and advanced technology for classified national security systems.
* Customer Service- Review detailed network architectures and provide specific guidance to improve security and mitigate risk during use, processing, storage, and transmission of information or data for Secretary of Defense Communications, Department of Homeland Security, White House Communications Agency, and Defense Information Systems Agency national security systems.

Selected Accomplishments:

* Led the architecture design, development, integration and test of the first classified mobile access communication infrastructure which significantly increased network security and mitigated defined risks.
* Established five cross-organizational teams to determine risks for commercial mobile attack vectors, delineated courses of action to mitigate the risks, and co-authored guidance for system owners.

**Senior Telecommunications Sciences Researcher, NSA** J Jan 2007- May 2013

GG15, 50 hours/week

Lead the wireless research team and research applications of software defined radios and wireless mesh networks.

Key Duties:

* Build the Team/Develop People – Guide research towards mission impact and strategic alignment.
* Innovate - Create an environment to generate research ideas, explore assumptions relevant to mission adoption, and jointly validate specific solutions with operationally focused organizations.
* Develop Mission Customers - Create research transfer opportunities for software defined radios on general purpose, field-programmable, and low-power processors and wireless mesh networking.
* Manage Budget - Garnered $M+ in funding annually to support continued research. Prioritize and execute research considering budget guidelines and constraints.

Selected Accomplishments:

* Consulted hundreds of hours on network vulnerability analysis of LTE (mobile 4G) throughout the Intelligence Community. Created and taught courses for nearly 800 people across 25 organizations, presented and moderated at Intelligence Community forums, and briefed NSA Advisory Board's CTO and Research Panels.
* Performed innovative research in wireless ad hoc networks, designed numerous routing algorithms, wrote over 8,000 lines of code implementing them into network simulators, developed hundreds of scenarios, and ran thousands of simulations to compare against established routing algorithms. Ultimately, earned U.S. Patent 8,443,103 for his routing algorithm which improved throughput by nearly 20% over established algorithms.
* Hosted and directed a multi-antenna conference and designed and built a next-generation multiple antenna system for operational purposes. Successfully deployed, the first of its kind in the Intelligence Community.
* Initial successes included fully cross-compiled modem functioning on development Smartphone, completed initial performance characterization, and demonstrated a running SDR modem performing survey/detect on a Smartphone.

**Software Engineering Leader, NSA** Feb 2004 - Dec 2006

GG14, 50 hours/week

Lead software development on tools to perform remote network operations.

Key Duties:

* Lead and Develop People – Guide software engineering towards mission impact and strategic alignment.
* Manage Software Development – Develop team vision, project schedules for software development, prioritized mission, and realigned resources for exploits to enable operational objectives.
* Enable Mission - Create standard operating procedures and training to reduce developer time required for remote operations.
* Manage Budget and Contracts - Prioritize and execute research light of budget guidelines and constraints.

Selected Accomplishments:

* Reduced delivery time of 9 software capabilities important to the Global War on Terror and eliminated need for 670 hours of operations support.
* Supported and promoted a new exploit development model which allowed more portability.

**Senior Mission Director, NSA** Aug 2002 - Jan 2004

GG14, 50 hours/week

Monitored and managed extremely complex dataflow system handling millions of files daily.

Key Duties:

* Lead and Develop People – Develop training and qualify new watch floor operators.
* Enable Mission – Monitor dataflow system health, proactively communicate detection of processing problems, and coordinate solutions, providing confidence in the operational data.

Selected Accomplishments:

* Modified and improved latency reporting software, allowing data quality assessment by senior operations personnel and other external customers during Operation Iraqi Freedom (OIF)
* Devised training vision for the operations center, developed Job Qualification Requirements training manual, revised standard operating procedures, and initiated the new certification process.

1999-2002 **US Naval Academy Leadership Course Developer and Instructor, US Navy**

1996-1999 **Patrol Squadron TEN** **P-3 Pilot, Flight Operations, Weapons/Tactics Expert, US Navy**

1992-1996 **Naval Flight Training, Navy Pilot, US Navy**

1994-1994 **University of Virginia Assist NROTC Instructor, Special Projects Officer, US Navy**