

## **XXXX XXXXXX**

000 I (Eye) Street, SW — Washington, DC 20024  
Home: (202) 000-0000 — White House: (202) 000-0000 — Mobile: (301) 000-0000  
Home: [xxxx@aol.com](mailto:xxxx@aol.com) — White House: [xxxx@who.eop.gov](mailto:xxxx@who.eop.gov)  
U.S. citizen — SSN 000-00-0000  
Highest Federal grade: GS-15 (current) — Veteran's status: US Air Force Officer (1981-92)  
Security clearance: **TOP SECRET/SCI with Polygraph**

**OBJECTIVE**            **Title**  
                              Agency  
                              Announcement number: **xxx**

### **PROFESSIONAL PROFILE:**

**White House Director of Cyberspace Security. Top-tier liaison across Defense and Intelligence Communities, Federal agencies, and private industry. Proven ability to lead complex projects and consistently deliver results. Broad experience on Joint Staff as a US Air Force officer. TS/SCI clearance with Polygraph.**

- Director of Cyberspace Security, Homeland Security Council, Critical Infrastructure Protection Office, The White House.
- Direct the implementation of the President's National Strategy to Secure Cyberspace. Coordinate with leaders at Federal, State and local levels. Plan and coordinate implementation of national-level policy and strategy to protect cyber assets in the Nation's critical infrastructure throughout government and industry.
- Senior liaison with the Intelligence Community to monitor cyber issues related to terrorism, including foreign-based hackers and nation states supporting these intrusions.
- Pivotal in establishing the National Cyber Security Division (NCSA) in the Department of Homeland Security. Coordinate with NCSA and industry to align national incident responses to cyber threats and intrusions.
- Served as NSA's Senior Corporate Alliance Manager. Identified areas where long-term alliances between NSA and industry would improve National Security by strengthening signals intelligence (SIGINT) and Information Assurance (IA).
- *"...irreplaceable asset...exceptionally strong skills in people management...has taken on a team marred with internal conflict and in jeopardy of missing critical deadlines, and formed a well-organized team...an enormous degree of initiative....gained significant productivity and reduction in costs..." (from official Evaluations)*

**Solid professional preparation. Broad intellectual perspective. Proven ability to build consensus and collaboration among groups pursuing diverse agendas.**

- MS in Management Sciences. BS in Mathematics.
- Graduate, National Senior Cryptologic course. Graduate, Wharton School of Business Executive Education in Strategic Alliances. Graduate, Federal Executive Institute.

## **DIRECTOR OF CYBERSPACE SECURITY**

Homeland Security Council — Critical Infrastructure Protection Office

The White House

Washington, DC

**Date:** 4/03 - present

**Grade:** GS-15

**Hours:** 50-65 per week

**Supervisor:** Ms. Frances Townsend — may be contacted

**Provide proactive, national-level strategic leadership for the conceptualization, planning, implementation and coordination of strategy and policy,** and their implementation, relating to the protection of cyber assets across the Nation's entire critical infrastructure.

- RESULT
- Direct a White House portfolio, working with top-tier leaders in the Intelligence Community to monitor cyber issues related to terrorism, foreign hackers, and nation states that may be supporting these threats and intrusions.
  - Responsible for seeing and presenting “the big picture” to White House decision makers including the Homeland Security Advisor and the National Security Advisor to the President. Prepare summary papers to explain the impacts of various cyber attacks or intrusions (i.e., virus, worm, Denial Of Service) on government and industry computer systems.
  - Instrumental in standing-up, establishing, and implementing the National Cyber Security Division (NCSD) within the Department of Homeland Security (DHS).

**Manage nation-wide resources as a member of Homeland Security Council working group** overseeing the DHS budgetary process. Primary responsibility for monitoring \$77.9M NCSD portion of the DHS annual budget. Ensure that NCSD's needs are convincingly articulated.

- RESULT
- Successfully advocated for—and received—an \$11M increase in NCSD's budget in an emergency supplemental funding bill.
  - Worked in close coordination with NCSD to coordinate national-level cyber incident response plans across government and industry. Got the first-ever Cyberspace Security Annex included in the National Response Plan (NRP).
  - Successfully advocated for—and received—additional \$3M in NIST, Commerce, and OSD budgets to support program proposals drafted under my direction. Each of these proposals implemented a recommendation in the President's National Cyber Security Strategy.
  - Successfully justified—and received—additional personnel resources to assist with cyber issues in specific sectors. Worked closely with senior leadership on the Homeland Security Council and White House Office for Personnel. Succeeding in getting two new Directors hired, both of whom have cyber security experience, with expertise in the financial sector and the legal field.
  - Praised for “*the network she has forged has proven invaluable in supporting her ability to carry out her assigned responsibilities especially in a high-pressure, time-sensitive environment...instrumental in laying the foundation for several of the NCSD's most successful partnerships.*”

**Build multi-organizational alliances and coalitions** with leaders at Federal, State and local levels, as well as the private sector, in overseeing implementation of the President's National Strategy to Secure Cyberspace.

- RESULT
- Primary point of contact within the White House regarding daily cyber activities.
  - Integrated the Chemical Sector's IT security efforts into overarching homeland security initiatives.
  - Raised awareness for more secure software and better security practices in the Chemical sector.
  - Educated vendors on the potential for hackers to use chemical facilities to create Weapons of Mass Destruction (WMD) in the United States.
  - Briefed CIOs from 60 chemical firms on the potential impact of a cyber attack in the Chemical sector, assisting them in drafting a cyber security strategy that aligned with the President's National Strategy to Secure Cyberspace.
  - Oversee the President's National Infrastructure Advisory Council (NIAC) and National Security Telecommunications Advisory Committee (NSTAC). Work closely with NIAC and NSTAC on various topics, including how we manage vulnerability disclosure across industry and the government.
  - Hosted meetings with members of European Commission, providing assistance in establishing the European Network and Information Security Agency.
  - Worked closely with Government of Japan in defining its role in cyber security, nationally and internationally.
  - Praised as *"consistently proactive ensuring that White House stakeholders, DHS and industry leaders have common goals....quick to take the lead....extremely successful at promoting cooperation between competing companies to improve this nation's defense posture in cyberspace security."*

**Co-Chair of a working group** to draft the implementation plan for National Security Presidential Directive (NSPD) 38—US Offensive Cyber Operations Policy.

- RESULT
- Drafted the portion of the Strategic Plan that addressed roles and responsibilities of each agency as well as interagency collaboration plans and mechanisms.

**Developed alignment among White House decision-makers and key staff** regarding the National Intelligence Priorities Framework (NIPF) and how it is intended to operate.

- RESULT
- Pulled together several DHS and White House cyber stakeholders.
  - Invited NSA to come to the White House to brief on the NIPF, with a focus on cyber threats.

**Defused potential organizational and media crises** through effective personal diplomacy.

- RESULT
- When the Director, NCSD, submitted his letter of resignation with only one day's notice, during the election campaign the night before the final debate, immediately set up a meeting with the Director to defuse this situation from becoming a "media feeding frenzy."

- Set up a meeting between Director, NCSD, and top DHS and White House officials to address major concerns of the outgoing Director—secured a promise by the Director to avoid negative press statements about his resignation.

### **SENIOR CORPORATE ALLIANCE MANAGER**

National Security Agency (NSA)  
9800 Savage Road — Fort Meade, MD 20755

**Date:** 1/02 – 3/03

**Grade:** GS-15

**Hours:** 50-60+ per week

**Supervisor:** Mr. John Nagengast

**NSA focal point for defining and building a long-term strategy** and corporate view of industrial alliances—leading to working relationships with private industry in key areas of National Security.

- RESULT
- Built a strategy for an intensive Corporate Outreach Plan to build new bridges and rebuild some old communication linkages between NSA and private industry.
  - Worked with industry and government partners to identify commercial technology trends, emerging technologies, as well as market leaders and corporate objectives.

**Liaison with Signals Intelligence (SID) and Information Assurance (IAD) Directorates** to identify areas where industrial alliances would strengthen the Directorates' respective missions.

- RESULT
- Developed a plan for the Director, enabling NSA to bring best practices and emerging technologies from private industry into NSA, to assist NSA in meeting its key challenges.

**Praised as a “change agent”**—drafted and coordinated implementation of NSA's first Corporate Governance Process.

- RESULT
- Developed a flexible process designed to accommodate and address security concerns between SID and IAD, and ensure that events and decisions are appropriately documented and actions are tracked accurately and effectively.

### **DEPUTY DIVISION CHIEF — POLICY, PROCEDURES AND COMSEC INSECURITIES**

National Security Agency (NSA)  
9800 Savage Road — Fort Meade, MD 20755

**Date:** 9/00 – 12/01

**Grade:** GS-15

**Hours:** 50-60+ per week

**Supervisor:** Thomas Dizubin

**Supervised a 35-person staff and three branches.** Reported to the Information Assurance (IA) Director for developing, coordinating, promulgating and ensuring the implementation of IA policies, internal and external, that support mission goals and objectives.

- RESULT**
- Successfully overhauled IA advisories and Technical Bulletins Program. Created and implemented the program's ability to support DoD Information Assurance Vulnerability Alert (IAVA) program, which most NSA staff had never heard of or understood, prior to my intervention.
  - Eliminated major confusion and duplications of effort among DoD customers of NSA, who were receiving vulnerability notices from DoD—through IAVA, with reporting instructions to ASD/C3I, and receiving NSA IA bulletins—with no guidance and no obvious connection between the two.
  - Provided direct support to the NSA CIO on NSA certification and Accreditation Plan—assisting CIO to better understand requirements of the DoD/Defense Information Technical Security Certification and Accreditation Process (DITSCAP) and how it translated into the Intelligence Community (IC).

**Developed and promulgated procedures** addressing the operation of fielded COMSEC equipment and IA products.

- RESULT**
- Managed the evaluation of COMSEC insecurities to include development and maintenance of databases and the preparation trend and analysis reports.

**CHIEF INFORMATION OFFICER (CIO)  
CHIEF — INFORMATION TECHNOLOGY AND ASSURANCE DIVISION**

Defense Information Systems Agency (DISA)

Office of the Chief Information Officer

3701 South Courthouse Road

Arlington, VA 22204

**Date:** 6/98 - 9/00

**Grade:** GS-15

**Hours:** 45-50+ / week

**Supervisor:** Shirley Fields (703) 696-1894 — may be contacted

**Planned and led Information Technology (IT) and Information Assurance (IA) strategy, policy, and procedures,** including implementation of existing and emerging IT and IA policy and procedural requirements for DISA as a central organization serving the Defense Community.

- RESULT**
- Ensured ongoing coordination and orchestration of DISA policy and procedures in this area with established DoD policy and objectives in the IT and IA areas.
  - Advised top management on significant multi-dimensional systemic issues and concerns that might affect effective synchronization of DISA and DoD policy and procedures in these areas.
  - Ensured that DISA's IT architecture was consistent with Defense Information Infrastructure (DII) and DoD architectures.

**Component Information System Security Manager for DISA**, responsible for developing and managing a DISA-wide Information Assurance program.

- RESULT**
- Established requirements and administer Information Security (INFOSEC) awareness, training and certification programs for all DISA employees.
  - Established and led uniform certification/accreditation program to implement DoD Information Technical Security Certification/Accreditation Process (DITSCAP).
  - Implemented and directed the DoD Information Assurance Vulnerability Alert (IAVA) across DISA. Maintained close liaison with Director of DISA and DAA regarding status of IA vulnerabilities and related risk factors.

**Senior Representative to Designated Approving Authority (DAA)**, who was also Chief Information Officer (CIO) and served as DISA's DAA Representative.

- RESULT**
- Recommended accreditation decisions based on comprehensive technical/non-technical security tests and evaluations and assessments of residual risk factors.

**Directed and coordinated** DISA's Webmaster-related responsibilities.

- RESULT**
- Directed content to be published. Defined criteria and oversaw DISA content managers to ensure protection of data published on DISA's Web pages.
  - Praised for "...*exceptionally strong skills in people management, project management and oversight...excellent technical knowledge and leadership in many areas of information technology...*"

## **CHIEF, SYSTEM SECURITY ENGINEERING DIVISION**

Defense Information Systems Agency (DISA)  
Joint Interoperability Engineering Organization (JIEO)  
701 South Courthouse Road — Arlington, VA 22203

**Dates:** 6/97 – 6/98

**Grade:** GS-1550-15

**Hours:** 55+ per week

**Supervisor:** Dr. Frank Perry — telephone unknown

**Performed dual managerial and technical responsibilities** for DoD security organizations: (1) DISA System Security Engineering Division, and (2) the NSA Network Security Group.

**Coordinated ongoing support to both groups** through their participation in the Joint Interoperability Engineering Organization (JIEO).

- RESULT**
- Ensured that both divisions possessed practical, cost-effective action plans to provide high-quality security engineering for DISA pillar programs: Defense Information Infrastructure Common Operating Environment, Defense Messaging System, Global Command & Control System, Defense Information System Network. Met all requirements, providing safe, cost-effective security engineering/architecture solutions for these key programs.

**Directed development of targeted security-related program management plans** for assigned organizations in both DISA and NSA.

- RESULT • Balanced available resources and assets to meet the multiple requirements of providing effective, cost-effective security engineering and architecture solutions to Department of Defense and Defense Community.

**Directed a \$35M annual operating budget and 30-person Information Security staff** of military and civilian engineers involved in Information Security (INFOSEC) activities.

- RESULT • Defined strategy for managing a complex series of independent engineering and program initiatives within both DISA and NSA.

**Directed the coordination of resources** for DISA's System Security Engineering Division and NSA's Network Security Group.

- RESULT • Balanced available resources and assets to meet multiple requirements—providing effective, cost-efficient security engineering and architecture solutions to DoD and the Defense Community.

**Provided technical leadership** on development and implementation of cutting-edge technologies supporting the new INFOSEC initiative.

- RESULT • Directed the development of technologies used in the following programs:  
DoD PKI (Public Key Infrastructure), ATM switch hardening effort, Secure Domain Name Service, and DII protect/detect/react Tools Program.  
• Praised as *“effective in opening up dialogue with other divisions....to present their security issues....expert in balancing available resources....”*

**LIAISON OFFICER — representing DISA to NSA**

Defense Information Systems Agency (DISA)  
701 South Courthouse Road — Arlington, VA 22203

**Date:** 11/94 – 6/97

**Grade:** GS-1550-15

**Hours:** 47+ per week

**Supervisor:** LTG Edmonds: (703) 607-6001 — may be contacted

**Liaison Officer on the Director's staff**, representing DISA to NSA to proactively promote the most effective working relationships between DISA and NSA

- RESULT • Personal Liaison to the Director, MSA, ensuring effective coordination and resolution of complex issues at Director level and throughout DISA and NSA.  
• Pivotal in building a key relationship between DISA and NSA, ensuring proper communication and dissemination of SCI intelligence through INTELINK-TS, as well as issues concerning who manages and provides Secret high intelligence information to warfighting organizations via INTELINK-TS and GCCS.

**Top-tier liaison with Directors of DISA and NSA** on a weekly basis, to discuss key concerns affecting both agencies.

- RESULT • Set up site visits between Directors of both agencies, their senior managers, and their Personal Liaison Officers.

**Recognized as technical authority and internal consultant on information systems**, working with the highest-ranking officials of both DISA and NSA to anticipate emerging problems and resolve existing problems.

- RESULT • Prepared and presented high-level briefings/reports to officials in DISA, NSA, and other components of the Defense Community, to explain and negotiate significant issues affecting nationwide information systems security issues.

**Coordinated both Directors' staffs** to generate support for a series of joint initiatives.

- RESULT • Coordinated joint support for the acquisition of commercial satellite communication capabilities and for the sharing of bandwidth, thus benefiting the mission performance of both agencies.

**Worked closely with DISA Program Managers and INFOSEC engineers in NSA**, coordinating a variety of technical issues affecting information systems and systems security.

- RESULT • Ensured appropriate level of security was being applied to programs such as: Electronic Commerce/Electronic Data Initiative (EC/EDI), DMS, and DISN.
- Praised for “*significant contributions...played a critical role throughout the writing and coordination of new Memorandum of Agreement (MOA) between DISA, NSA and the Defense Intelligence Agency...instrumental in resolving all concerns before the MOA was signed by the three agencies' Directors...*”

## **COMPUTER SCIENTIST**

Defense Information Systems Agency (DISA) — APS11, Room AE209  
9800 Savage Road — Fort Meade, MD 20755

**Date:** 1/93 – 11/94

**Grade:** GS-1550-14

**Hours:** 40-50+ per week

**Supervisor:** George Sutherland: (410) 859-4515 — may be contacted

**Selected for assignment to joint DISA/NSA Directorate** onsite at NSA. Consolidated and defined security policies, established standardized formats for system security requirements, and sound security architectures to meet goals established by DoD Goal Security Architecture (DGSA).

- RESULT • Served on the team that wrote the DGSA document. Provided guidance to users and vendors on implementing the DGSA.

**Security Architecture Test and Evaluation Program Manager**, working in DISN-NT SPO (DISN-Near Term Special Program Office), responsible for management, oversight, and

accountability of the development, acquisition, and fielding of DISN-NT Security Architecture.

- RESULT** • Coordinated all formal accreditation activities for DISN-NT with DISN Security Accreditation Working Group (DSAWG)—ensured that all system components were thoroughly tested and a security profile was completed on each element.

**Directed the coordination of technical system elements** into overall system architecture capable of being used by senior staff members in the joint DISA and NSA Directorate.

- RESULT** • Coordinated the integration of all components into the Laboratory. System integration and security testing of pilot prototype system, ensuring its effectiveness.

### U.S. AIR FORCE CAREER: 1981-1992

#### **SECURITY OFFICER**

US Air Force — assigned to DISA, Defense System Support Organization (DSSO)  
The Pentagon — Washington, DC 20301

**Date:** 12/90 – 12/92

**Grade:** Captain

**Supervisor:** LCDR Spraitzar (telephone unknown)

**Hand-picked by Vice Director, Joint Staff** as ADP System Security Officer serving over 6,000 users of Worldwide Military Command and Control System (WWMCCS).

- RESULT** • Focal point of all security issues for WWMCCS Intercomputer Network (WIN). Kept DAA informed, making recommendations on security incidents that could cause a site to be denied network access.

**Coordinated WIN computer connectivity** with numerous DoD organizations, including NSA, the Office of the Secretary of Defense, HQ US Marine Corps, and Defense Nuclear Agency.

- RESULT** • Provided critical automated input to senior decision-makers across DoD.

#### **REQUIREMENTS ANALYSIS / MANAGER**

US Air Force — assigned to DISA, Defense System Support Organization (DSSO)  
The Pentagon — Washington, DC 20301

**Date:** 12/88 – 12/90

**Grade:** Captain

**Supervisor:** Ms. Shipp (telephone unknown)

**Branch ADP expert** maintaining the overall DSSO computer requirements process.

- RESULT** • Analyzed, designed, coded and implemented an ORACLE Tracking and Suspense System throughout DSSO to monitor and maintain all DSSO actions, and to provide senior leaders with status reports.

**Coordinated IT requirements** with the Joint Staff, OSD and WWMCCS sites.

- RESULT**
- Provided key feedback to senior decision-makers across DoD on a variety of issues in this area.
  - Managed WIN connectivity for operation support of the DIA Crisis Management Team during the Gulf War.
  - Managed WWMCCS remote terminal upgrade and NMCC port connectivity issues for HQ, Marine Corps, ending reliance on ineffective manual methods and providing an automated capability with proper security levels.

**Supervised reviews of security audit information**, serving in a liaison capacity to share and implement this information.

- RESULT**
- Liaison Officer between DSSO and user communities and their action officers, providing expert technical advice for their long-range planning.
  - Managed a \$50K contract to improve system audit capabilities of nine (9) highly classified and sensitive computer systems supporting DoD agencies.

### PRIOR POSITIONS

#### **NAVY CRUISE MISSILE SYSTEM ANALYST**

1987-88 — Washington Navy Yard — Washington, DC

**Configuration Management Officer and troubleshooter**, working with System Software Test and Evaluation Team for this Joint Service initiative.

- RESULT**
- Verified and evaluated complex computer systems used on nuclear ground and sea-launched Cruise Missiles.
  - Replicated system discrepancies reported by users at other sites, clarifying problem-set for programmers to generate effective solutions.
  - Developed and wrote end-to-end test plans for the latest software being used at these test sites.
  - Chair, Configuration Engineering Review Board.
  - Chair, Internal Review Board.

#### **BRANCH CHIEF, SATELLITE SOFTWARE SUPPORT**

1982-1987 — Eglin AFB — FL

**Directed three programming teams** and an 18-person technical staff.

- RESULT**
- Directed the management and enhancement of 300+ programs involved in satellite tracking software.
  - Identified and resolved software problems to restore missile warning AN/FPS-85 Phased Array Radar to operational capacity—restoring missile warning capabilities for a system serving as a direct backup for Cheyenne Mountain.

EDUCATION — ADVANCED PROFESSIONAL TRAINING

**MS, Management Sciences, 1987**

Troy State University — Troy, AL

**BS, Mathematics, 1981**

Fayetteville State University — Fayetteville, NC

National Cryptologic Course, 2002

Wharton School of Business Executive Education — Strategic Alliances, 2002

Federal Executive Institute, 1998

Understanding and Using Malcolm Baldrige Criteria, 1997

Computer Technical Training School — US Air Force, 1981-82

AWARDS — RECOGNITIONS

Women of Cyber Security Award — Women's High-Tech Coalition — 2004

Outstanding Performance Cash Awards, 2000, 1999, 1998, 1997, 1996, 1995, 1994, 1993

Outstanding Young Woman of America Award, 1988

NAACP Citizenship Award, 1977

NAACP Academic Award, 1977

Numerous military awards throughout US Air Force career

ACTIVITIES

Volunteer tutor in Mathematics — public school students in the Washington, DC area

Active member — Tuskegee Airmen, Inc.

SIGNATURE

I certify that, to the best of my knowledge and belief, all of the information on and attached to this application is true, correct, complete and made in good faith. I understand that false or fraudulent information on or attached to this application may be grounds for not hiring me or for firing me after I begin work, and may be punishable by fine or imprisonment. I understand that any information I give may be investigated. You are hereby authorized to contact my present supervisor.

Signature: \_\_\_\_\_

Date signed: \_\_\_\_\_

