**Houman Hadaegh**

Mobile: (301) 602-0708

Email: [houmany@gmail.com](mailto:houmany@gmail.com)

<https://www.linkedin.com/in/houmanh/>

**SUMMARY**:

Detail-oriented executive leader with 20 years of expertise in IT infrastructure projects and security management for defense, civilian, and commercial clients. A Level 5 leader as coined by Jim Collins, with a professional philosophy based on the pillars of empathy, commitment, discipline, resiliency, and integrity.

* Leads and delivers highly technical, innovative solutions to the federal sector in the realms of cybersecurity and cloud computing.
* Develops technology initiatives that optimize operations, align with business objectives, and promote growth capabilities.
* Provides strategic direction and oversight for the design, development, operation, and support of IT systems and programs that fulfill business needs, including enterprise architecture management, application management, security and risk management, and infrastructure and operations support management.
* Advises senior executives on their overall technology strategy and leads its execution; engages teams and works collaboratively across departments to proactively solve problems, build consensus, and deliver critical projects.
* Technical specialties include security architecture and program development, risk management, vulnerability management and assessment, incident response, and policy development. Vast experience with NIST Publications, DOD Instructions/Directives, OMB Circulars/Memoranda, FISMA, PCI DSS, ISO/IEC 27000, 20000 series, and ITIL frameworks.

# SECURITY CLEARANCE:

DoD Top Secret

# CERTIFICATIONS:

* Project Management Professional (PMP) - Number: 1333520
* Certified Information Systems Security Professional (CISSP) – 337761
* ITIL V4

# EMPLOYMENT HISTORY:

**Chief Technology/Information Security Officer, October 2015 - Present**

Employer: IBSS Corp

For the past five years, led the strategic vision for the IT services and capabilities. Developed a one-year, three-year, and five-year roadmap for IT capabilities and strategies across cybersecurity, enterprise infrastructure, and cloud computing verticals. This involves reviewing the latest technologies from industry leaders and engaging with clients to discuss their technical challenges and goals. Internally, led the establishment of departmental performance goals, objectives, and operating procedures with KPIs that produce measurable results within budgets and timeframes. Played a key role in standing up IBSS’s PMO to provide oversight of project and quality management for a diverse set of federal clients in IT, Scientific Engineering and Management Consulting services. Co-led IBSS to achieve externally-certified ISO 9001, ISO 20000, ISO 27001, and CMMI-SVC/ML3 processes to deliver secure IT services across federal clients. Led IBSS in winning opportunities, providing technical solutions to client needs, capture management of key personnel, and proposal development for $34 million in IT services in the past ten years.

**Program Manager/Enterprise Architect, October 2009 - 2019**

Employer: IBSS Corp

***Client:*** *DoD Education Activity (DoDEA) OCIO - 2009 – 2019*

Served as a Technical Program Manager/Enterprise Architect and strategic advisor to DoDEA CIO, CTO, and CISO. I managed and provided leadership to a cross-functional team of network, system and security engineers with an operational budget of $35M with 35 direct reports and 42 indirect reports across the global enterprise in the Americas, Europe, and Pacific theaters. Responsibilities encompassed the development and maintenance of the agency’s Information Security Program and technical oversight for 90,000+ users worldwide across Commercial, Non-Secure Internet Protocol Router Network (NIPRNet), and Secret Internet Protocol Router Network (SIPRNet) enclaves.

Developed and presented overall strategy, mission, and key performance indicators for Cyber/Information Security Operations within DoDEA ecosystem in support of the CIO and CTO vision. Developed short-term and long-term strategic roadmaps providing leadership and direction for the enterprise cyber/information security operations/program. Maintained an in-depth understanding of current and emerging information security, regulatory, and compliance trends as they relate to the DoD and NIST technology services. Supervised the design, implementation, maintenance, and performance of information security controls for the organization's networks, information systems, and critical assets. Lead the development and implementation of effective and reasonable policies and practices to secure protected and sensitive data and ensure information security and compliance with relevant legislation and legal interpretations. Lead efforts to internally assess, evaluate, and make recommendations to senior executives regarding the adequacy of the organizations' information and technology systems' security controls. Worked with DoD leadership and relevant responsible compliance department leadership to effectively build cohesive security and compliance programs for the organization to address federal statutory and regulatory requirements.

Successfully led 30 DoDEA information security efforts, from cloud security design and management, to policy auditing, to anti-virus solution and host-based intrusion prevention system design and implementation. My team integrated cutting edge security technologies that implemented a defense in depth architecture and continuously monitor and provide timely response to security events for over 100,000 global endpoints to protect the IT resources of 15,000 employees serving 73,000 students across 168 schools in 12 countries.

* Successfully lead the initiative to consolidate seven enterprise datacenters covering CONUS and OCONUS into a single Global Datacenter with an enhanced and optimized security stack located in Peachtree City, GA.
* Lead DoDEA’s transition to Risk Management Framework (RMF) from DoD Information Assurance Certification and Accreditation Process (DIACAP) based on DoDI 8510.01 guidance and through analyzing risks and recommending common controls; developing review processes and documentation templates that support RMF methodology, and developing and implementing a cybersecurity assessment plan for the DoDEA CIO. Assessed the status of DoDEA’s DIACAP implementation, and migrated DoDEA’s 25 Major Applications (MA) and General Support System (GSS) Enterprise Mission Assurance Support Service (eMASS) packages to RMF.
* Lead the enhancement of DoDEA’s defense-in-depth perimeter security architecture by migrating from Cisco 5520 ASAs to a highly available Palo Alto 5060s next-generation firewalls at each Internet Access Point (IAP) located in Georgia, Sembach and Okinawa. Standardized and configured SSL decryption, malware protection, intrusion prevention, URL Filtering, and WildFire sandboxing.
* Provided technical oversight and management on multi-tier architecture and deployment of enterprise monitoring solutions for 20,000+ network devices using SolarWinds NetFlow Traffic Analyzer & Network Performance Monitor to provide performance, availability, and fault monitoring capabilities. We developed dashboards that provide meaningful and simple-to-understand performance statistics to upper management and NOC/SOC engineers and analysts. Benefits resulted in reduced time spent on identifying, analyzing, and troubleshooting infrastructure issues.
* Provided technical oversight and management on standardizing DoDEA’s MS Active Directory (AD) domain structure and architecture to enhance the security posture of the organization. DoDEA’s single global forest has just under 500k AD objects, close 900 GPOs, and operates in a very large network of over 100 sites with over 100 domain controllers across the United States and other countries. Established a framework for consolidation of many domains into a few AD domains and a structured centralized AD management model, which offered the advantages of automatic trusts, common catalog, schema, and configuration changes applied once and synchronized throughout all domains that are part of the forest.
* Provided technical oversight and management on the implementation of McAfee ePolicy Orchestrator (ePO) architecture that was strategically deployed throughout the enterprise to ensure up-to-date Host-Based signatures protect the agency’s assets. Utilized McAfee Host Intrusion Prevention System (HIPS) to detect and block known intrusion attempts and creates custom rules to mitigate against Zero-Day attacks. Threat data was compiled and analyzed by dedicated intrusion-analysis SME’s who provide a weekly brief of enterprise security status. In addition, Policy Auditor (PA), Rogue System Detection (RSD), and Data Loss Prevention (DLP) modules were deployed across the enterprise for more than 100,000+ nodes to enhance DoDEA’s cyber hygiene.
* Provided technical oversight and management on the implementation of McAfee Enterprise Security Manager (ESM) for real-time visibility into all activity on all systems, networks, databases, and applications for 10,000+ nodes (network devices and servers). Deployment of this solution resulted in streaming security operations, providing a centralized view of an organization’s security posture, compliance status, and prioritized incidents that require investigation.
* Led the initiative to enhance DoDEA’s vulnerability management program by the enterprise deployment of Tenable Network Security Named Assured Compliance Assessment Solution (ACAS). DoDEA’s ACAS architecture is divided into four geographic areas – HQ, America, Europe, and Pacific. Each area has a SecurityCenter managing some number of scan zones within its sphere of influence. The solution provided a centralized view for all network activity, including asset discovery, vulnerability detection, configuration and compliance auditing, and event management.
* Managed communication and stakeholder engagement to include; business intelligence; outreach to the stakeholder community; creation and updating of briefing packages and technical and operational guidance documents for upper management; on-going formulation, tracking, and reporting for internal and external data calls, e.g., CCRI audits, and CyberScope.
* Lead the development and implementation of a DoDEA wide Policy Remediation program based on DoD, CNSS, NIST, and OMB compliant security policies to assist in the closure of CCRI and FISMA audit recommendations.

**Client**: NOAA OCIO Network Operation Center Support – 2010 - 2013

* Provided project management for an average workload of 13 simultaneous infrastructure projects at remote locations throughout the US.
* Delivered processes included: Change Management, Incident Management, Infrastructure Decommissioning, and Server and Firewall Requests Processes.
* Conducted and documented numerous "deep dive" interviews with engineers, IT security analysts, project managers, and IT consultants to develop an in-depth understanding of current configurations and processes in preparation for data center process builds.
* Reviewed blueprint engineering assessments, produced sizing analysis, project documents, coordinated project schedules, and ran virtual war rooms for infrastructure implementation.

**Client**: NOAA OCIO Web Operation Center Support - 2010 – 2013

Using PMI/PMBOK principles, developed and managed project plan (scope, business case, risk plan, schedule/timelines, dependencies, constraints, budget, stakeholder's management plan, communications plan, RACI, prepared all project documentation; facilitated project meetings; prepared presentations; worked with cross-functional teams; managed onsite/external vendors; followed Change Control, IT Security and IT Compliance policies and procedures.

**Senior IT Consultant, March 2006 – October 2009**

Employer: Booz | Allen | Hamilton

**Client**: U.S. Air Force

Lead a team of developers and network engineers that were responsible for designing a Base Decision Support System (BDSS) for the United States Air Force under the Biometrics Task Force. The AF BDSS was an initiative to improve current identity management and security practices such that changes in suitability status can be acted upon in a timelier manner.

* Designed and deployed Federation and Single Sign-On (SSO) technologies across two entities using different COTS products.
* Engaged with designing, installing, and configuring Microsoft (MS) Active Directory (AD), MS AD Federation Services (ADFS), CA SiteMinder Web Access Manager and CA Identity Manager.

**Client**: U.S. Department of the Treasury

* Supported was an IdAM Concept of Operations (CONOPS) for the Department of Treasury. The CONOPS illustrated a 3-5-year operating model that enables the development of the IdAM future state vision and expectations into an operational concept that drives requirements across process, organization, and technology. It articulated a Treasury IdAM business vision and provided the ability to develop a strategic plan. It also allows Treasury to communicate a shared IdAM vision to both internal and external customers and facilitates organizational buy-in and ownership for a Treasury IdAM program from its bureaus.
* Defined and documented the application security architecture for project solutions as part of the SDLC process and provided input and governance to the SDLC process.
* Participated in IT strategy planning activities, bringing a current knowledge and future vision of security technology, and how they interact with the Treasury application portfolio and business goals and objectives.
* Provided hands-on experience in conducting C&A activities, which included developing security requirements, developing artifacts, conducting security tests and evaluations, developing risk assessments, and documenting the information system in system security plans through all accreditation activities.
* Developed and updated department-level IT security policies, procedures and plans such as PII/sensitive information handling, risk management, incident handling, contingency planning, secure backup and recovery, account management, personnel security, physical security and rules of behavior.
* Performed collaborative reporting on operational security service levels, security event correlation strategy, intrusion prevention system enhancements, identification of security gaps, security enhancement planning, and project-based timeline metrics.

**Client**: Defense Information Systems Agency

* Managed a technical team of 10 security personnel to create an integrated approach that provides data integrity, information confidentiality, and service availability.
* From a strategic perspective, implemented security best practices and helped drive compliance in a number of key business areas, including DOD/federal security compliance, industry regulation/standards, and compliance frameworks
* Ensured that risk analysis methods are embedded across architectural programs as new technologies and solutions are implemented.
* Designed, analyzed, and implemented security essential practices and infrastructure at the data, application, service, operating system, and network levels to safeguard all data center assets and data.
* Focused on application security, intrusion detection, vulnerability assessment, proactive network monitoring and protection, and participated in systems development and deployment decisions from the perspective of security best practices.
* Reviewed security measures including SIEM, DLP, IPS/IDS, AV/malware, DRP/BCP, MDM, endpoint protection, software updates, physical security, and all controls, policies, and procedures. Presented findings in presentations to executives and technical teams.

**Senior IT Engineer, June 2000 – Feb 2006**

Employer: IBSS Corp

**Client**: National Oceanic and Atmospheric Administration OCIO

* Designed and implemented a MS Windows 2003 based Active Directory migration from Windows NT for 1000 users and over 60 servers that covered us of highly available Domain Controllers (DC), DNS, DHCP, Print, File Sharing and Web services architectures.
* Created various complex and advanced group policies and organizational units to improve the security and administration of the organization.
* Established various IT policies and automation procedures which included the implementation of MS Operations Manager (MOM) 2005 for server monitoring and MS Systems Management Server (SMS) for software deployments, password synchronization, automated critical patch deployment and self-service password reset.
* Assisted with the modernization of a Wide Area Network (WAN) of 35 sites nation-wide utilizing Cisco routers (2500, 2600, 3600 and 3700) and MCI frame and relay cloud.
* Configured and maintained varied Cisco equipment such as Catalyst 6500 Layer 3 core switches with Firewall Service Modules, Catalyst 4000 and 3500 access switches, 2600 and 3600 routers and VPN Concentrators.
* Assisted in the design, configuration, and implementation of Cisco Access Control List (ACL) on all WAN routers to secure the WAN and to protect the remote Local Area Networks (LAN)’s from attacks.
* Assisted in headquarters LAN upgrade by designing and configuring Cisco Gigabit Ethernet as backbone using various Cisco Catalyst switches. Configured a new set of IP addressing schemes to create different Virtual LANs (VLANs) to provide security, bandwidth management and traffic control.
* Installed and configured Multi Router Traffic Grapher (MRTG) to monitor the bandwidth usage for individual remote offices. In addition, installed and configured Big Brother software to monitor the operation of all devices and to notify the administrators if an outage occurs.
* Designed and implemented Network-based Intrusion Detection Systems (NIDS) to detect Denial of Services and Prob&Scan attacks, both on testbed network and enterprise network.
* Constructed vulnerability analysis and penetration testing for both wired and wireless networks, providing security by Cisco firewall, NIDS, Snort, and TippingPoint IPS. More than 10 kinds of Distributed Denial of Service and probing & scanning attacks were used for evaluation.
* Designed and implemented a novel authentication scheme (RSA-based), for a distributed system (wireless Mobile Ad hoc Networks) for two-factor authentication of network devices.
* Configured IDS alerts correlation and analysis for finding cooperative scans and reducing false positives.
* Reviewed all-source intelligence information and correlated it with data derived from various levels of perimeter defenses architecture (IDS, Firewalls, and Logs) to provide the customer with assessments and reports facilitating situational awareness and understanding of the current cyber threat.

# EDUCATION:

**University of Maryland, College Park** 2004

B.S. Degree, Electrical Engineering

**University of Maryland, University College** 2018

B.S. Degree, Cybersecurity

# KNOWLEDGE AND TECHNICAL SKILLS:

|  |  |
| --- | --- |
| **Federal Policies** | NIST Publications, DOD Instructions/Directives, OMB Circulars/Memoranda, FISMA, PCI, HIPPA, SOX, ISO/IEC 27000 series, ITIL |
| **Federal Audits** | DISA Command Cyber Readiness Inspections (CCRI) and FISMA |
| **Information Security Operations** | Assessment and Authorization, Business Continuity/Disaster Recovery Planning, Risk Management, Risk Analysis, Continuous Monitoring, Vulnerability Assessments, Threat Assessments, Incident Response Planning, Change Configuration Management, Security Architecture Analysis, and Security Compliance |
| **Information Security Tools** | McAfee Host Based Security System (HBSS), Tenable Assured Compliance Assessment Solution (ACAS), Palo Alto Firewalls, McAfee Enterprise Security Manager (SIEM) |
| **Operating Systems** | MS Windows 2012 and 2016 |
| **Applications** | MS Active Directory |
| **Networks** | Routers, Switches, Firewalls, IPS/IDS, Network Access Controllers, Wireless Lan Controllers, SSL & IPSEC VPNs |
| **Cloud Platforms** | Amazon Web Services (AWS), Microsoft Azure Cloud Services, Google Apps for Business, FedRamp |
| **Virtualization** | VMware ESX/ESXi, Microsoft Hyper-V |
| **Storage** | EMC Data Domain |
| **Backup** | BackupExec and NetBackup |