IT Security Specialist IT Security Specialist IT Security Specialist - Richard S. Carson & Associates, Inc Ms. Ntinglet is a dedicated, focused, and extremely knowledgeable Senior IT Security Analyst. As an experienced information system security professional, I bring over Seven (7) years of comprehensive IT Security leadership and support experience. During my two-year tenure with the Enterprise-Wide Security Services Compliance (EWSSC) contract, I have directly supported the NOAA and NIH OCIO Risk Management Framework initiative. In this capacity, my knowledge, experience and meticulous approach to IT Security compliance has directly contributed to the enhanced protection of NOAA information systems. Assisted NOAA and NIH IT Risk Manager in coordinating the IT Security Program and disseminating IT Security information, requirements, and policies throughout NOAA and NIH. Examples of my subject matter expertise and genuine understanding of the security process include the preparation of Security Authorization packages in accordance with National Institute of Standards and Technology (NIST), Federal Information Security Management Act (FISMA) and other Federal Government requirements. Work Experience IT Security Specialist Richard S. Carson & Associates, Inc August 2017 to Present Responsibilities: As an IT Security Specialist at NIH, Ms. Ntinglet's responsibilities required an outstanding level of professional knowledge of Information Technology Security Specialist and skill in and security-related reporting. Her responsibilities include the following: Senior Cybersecurity Analyst Fusion PPT March 2017 to July 2017 Responsibilities: As a Cybersecurity Analyst at NIH, Ms. Ntinglet's responsibilities required an outstanding level of professional knowledge of cybersecurity and skill in data analysis and security-related reporting. Her responsibilities include the following: Creating, revising, and reviewing System Security Plans (SSP), Security Assessment Plans (SAP), Plan of Action & Milestones (POA&M), Security Assessment Reports (SAR) for low, moderate and high systems and additional documentation. Conducting full life-cycle A&A assessments as well as Security Control Assessments. Assisting with the transition from C&A or SA&A to A&A and NIST 800 series. Assisting with compliance reviews and documentation for new or noncompliant systems including FIPS-199 system categorizations, E-Authentication risk assessments, Privacy Threshold Assessment, Privacy Impact Analysis, and Security Controls Assessments. Applying the National Institute of Standards and Technology (NIST) Special Publications and FIPS as a framework for conducting A&A activities on federal IT systems. Updating Federal policies, regulations, FISMA compliance and standards, and cybersecurity requirements. Assessing for and maintaining compliance within Federal Standards such as NIST SP 800-53A rev. 4 and NIST SP 800 53 Rev 4. Performing security assessments of all security controls within the network. Working with the Federal ISSOs to complete A&A artifacts including System Security Plans, Configuration Management Plans, Business Impact Analysis, Business Continuity Plans, and supporting the ATO process. Providing cybersecurity technical advisory services regarding Federal and commercial leading practices, relevant strategic initiatives, and emerging technologies/trends. Understanding compliance requirements, standards, and guidelines governing security within the Federal Government including FISMA, OMB Circular A-130, FIPS 199, FIPS 200, and the NIST Risk Management Framework. Understanding NIST Special Publications; specifically, 800-30 rev 1; 800-37 rev 1; 800-39; 800-137; 800-34; 800-60 rev 1, Volumes 1&2, 800-18 rev. 1; 800-88 rev 1; 800-137; and 800-128. Accomplishments: I completed conducting SA&A/Risk Assessments, IT Security Compliance and Testing before deadline. IT Security Analyst Maximus 2011 to 2017 Responsibilities: Lead, manage and update the organization's security control assessment from NIST 800-53 A rev1 to 800-53A rev4. Has developed a Power- point presentation on upgrade from NIST SP 800-53 Rev 3 to Rev 4 and presented it at the Cyber Security Conference this year. Communicate with client-facing Information Assurance support as an Information System Compliance Analyst to the National Oceanic Atmospheric Administration (NOAA) Enterprise-Wide Security Services Compliance (EWSSC) Team Analyze the organization's 118 Low, Moderate, and High systems for security compliance with NIST SP 800 series documents, FISMA, and OMB standards and regulations based upon a Risk Management Framework and thorough understanding and knowledge of SA&A process. Analyze High Impact Systems' Authorization to Operate (ATO) compliance packages to help support the Chief Information Officer (CIO) in critical business decisions of operations and continuous monitoring A&A Coordination: Perform documentation review in alignment with the NOAA/IA quarterly memo.

Verify NOAA/IA issued POA&M grades in quarterly memo for accuracy. Privacy Impact Assessment: Provide support to ISSO to edit and complete PIAs through the Department Privacy Division. Attend weekly POA&M Corrective Action Meetings to implement recommended risk mitigation strategies. Developed, implemented, managed, and reported on security policy's, SOPs, and guidelines based on NIST, DOC and NOAA. Utilize CSAM to generate systems security analysis reports, plans, and continuous monitoring documents and assist in providing user provisioning support for CSAM. Perform Continuous Monitoring and IA program assessments analysis and activities. Lead in developing Agency Templates and conduct annual compliance reviews for Security Assessment Reports (SARs), Review authorization documentation for completeness and accuracy for compliance with departmental policy. Analyze and advise compliance-level recommendations for system documents such as (e.g., System Security Plan, Contingency Plan, Privacy Impact Analysis, Security Control Assessment, Business Impact Analysis, Risk Assessment Report, Security Assessment Results, etc.). Accomplishments: I completed the required project given to me ahead of deadline commendations from customers/clients also receive pats on my back from my supervisor and token from my company as well. State and Federal 2014 to 2014 Will establish and maintain information security policies, procedures, and guidelines pursuant to the HHS, NIH and NIGMS requirements, as well as, State and Federal laws and regulations such as the Federal Information Security Act (FISMA) 2014. Performs and prepares SA&A documentation on NIH systems based on guidance from NIST SP 800 series, FIPS 199, OMB Guidance, Federal law, and HHS and NIH policies and guidance. Documentation includes security plans, risk assessments, contingency plans, and security test and evaluation (ST&E) plans and reports for major applications and general support systems (GSS) including the NIHnet backbone. Provides recommendations for security controls to enhance the overall security posture of the network. Performs privacy impact assessments (PIA) on NIH systems for accuracy and performs security impact assessments to evaluate the effects of system changes. Will manage the information security function in accordance with the established policies and guidelines. Conduct and perform continuous monitoring pursuant to NIST Guidelines and

NIGMS OCIO requirements. Accomplishments: Completed interviewing point of contacts and wrote up the results in NSAT. Education M.S in Information in Security/Assurance Capella University 2010 to 2012 M.A in Counseling in Counseling University of the District of Columbia 1995 to 1997 B.S in Public Health Education in Public Health Education University of the District of Columbia 1989 to 1992

Name: Donna Collins

Email: hbrown@example.com

Phone: (685)743-4891