Project Name: Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services

TABLE OF CONTENTS

12/15/2023 - U.S. Air Force Information Technology (IT) Lifecycle and Performance System

Contract Name	Customer Name	Customer POC	Total Contract Value	Period of Performance	Is there a CPARS available?
Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services to the National Center for Health Statistics (NCHS)	Centers for Disease Control & Prevention (CDC)	Avay Dolberry, COR aym6@cdc.gov 919-541-2700	$1,585,530.9	07/03/21 - 01/02/26	Yes
Description of Services: RELI Group supports the NCHS ISSO in delivering information security services, guidance, and training to CDC information security stakeholders (e.g., business owners, security analysts, system developers, and other business partners) in the areas of cybersecurity risk and compliance management, Security Assessment and Authorization (SA&A) audit analysis and support, software assurance, security awareness training, incident response, contingency planning, and policy implementation. RELI Group also supports all security-related documentation and activities, interprets regulations and policy guidance, develops training materials, provides strategic support in attaining/maintaining NCHS information systems' ATO, and includes risk analysis and advice, secure baseline configuration guidance, and security tool training and support. Their services also include analyzing all NCHS SA&A documentation submitted for Annual Assessments and ATO pursual/renewal efforts, including Systems Security Plans (SSP), Privacy Impact Assessments (PIA), Business Continuity Plans (BCP), and other related system documentation. They evaluate SA&A packages and related documentation (e.g., SSPs, PIAs, BCPs), providing analysis and guidance to system developers and maintainers regarding identified findings, architectural gaps, and policy/process deficiencies. RELI Group also assists in audit coordination, responding to requests for information from auditors, tracking the weakness remediation process, and resolving POA&M by regular communication with system owners and system security personnel.					

10/06/2023 - U.S. Air Force - Enterprise Security Services RFI

Contract Name	Customer Name	Customer POC	Total Contract Value	Period of Performance	Is there a CPARS available?
Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services to the National Center for Health Statistics (NCHS)	Centers for Disease Control & Prevention (CDC)	Avay Dolberry, COR aym6@cdc.gov 919-541-2700	$1,585,530.9	07/03/21 - 01/02/26	Yes

Description of Services: RELI Group supports the NCHS ISSO in delivering information security services, guidance, and training to CDC information security stakeholders (e.g., business owners, security analysts, system developers, and other business partners) in the areas of cybersecurity risk and compliance management, Security Assessment and Authorization (SA&A) audit analysis and support, software assurance, security awareness training, incident response, contingency planning, and policy implementation.

RELI supports all security-related documentation and activities, interprets regulations and policy guidance, develops training materials, provides strategic support in attaining/maintaining NCHS information systems' ATO, and includes risk analysis and advice, secure baseline configuration guidance, and security tool training and support. Our services include performing analysis of all NCHS SA&A documentation submitted for Annual Assessments and ATO pursual/renewal efforts, including Systems Security Plans (SSP), Privacy Impact Assessments (PIA), Business Continuity Plans (BCP), and other related system documentation. We evaluate SA&A packages and related documentation (e.g., SSPs, PIAs, BCPs, etc.), providing analysis and guidance to system developers and maintainers regarding identified findings, architectural gaps, and policy/process deficiencies. We also assist in audit coordination, responding to requests for information from auditors, tracking the weakness remediation process, and resolving POA&M by regular communication with system owners and system security personnel.

08/17/2023- Department of the Army Cybersecurity Policy Support Services

Customer	**Contract Name**	**Total Contract Value**	**Period of Performance**
Centers for Disease Control & Prevention (CDC)	Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services to the National Center for Health Statistics (NCHS)	$1,585,531	7/3/2021 - 1/2/2026

Description of Services: RELI Group supports the NCHS ISSO in delivering information security services, guidance, and training to CDC information security stakeholders (e.g., business owners, security analysts, system developers, and other business partners), in the areas of cybersecurity risk and compliance management, Security Assessment and Authorization (SA&A) audit analysis and support, software assurance, security awareness training, incident response, contingency planning, and policy implementation.

RELI supports all security-related documentation and activities, interpretation of regulations and policy guidance, develops training materials, provides strategic support in attaining/maintaining NCHS information systems' ATO, and provides risk analysis and guidance, secure baseline configuration guidance, and security tool training and support. Our services include performing analysis of all NCHS SA&A documentation submitted for Annual Assessments and ATO pursual/renewal efforts, including Systems Security Plans (SSP), Privacy Impact Assessments (PIA), Business Continuity Plans (BCP), and other related system documentation. We evaluate SA&A packages and related documentation (e.g., SSPs, PIAs, BCPs, etc.), providing analysis and guidance to system developers and maintainers regarding identified findings, architectural gaps, and policy/process deficiencies. We also assist in audit coordination, responding to requests for information from auditors, tracking the weakness remediation process, and resolving POA&M by regular communication with system owners and system security personnel.

06/08/2023 – NIH NIAIDS

Contract Name & Number	Customer Name	Total Contract Value	Number of FTEs	Client POC Information	Is there a CPARS available?
Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services to the National Center for Health Statistics (NCHS)	Centers for Disease Control & Prevention (CDC)	$1,585,531	1.5	Avay Dolberry, COR 919-541-2700 aym6@cdc.gov	Yes
Description of Services: RELI provides cybersecurity consulting services to the Centers for Disease Control and Prevention’s (CDC) National Center for Health Statistics (NCHS), assisting the NCHS Information Systems Security Officer (ISSO) in meeting the information security and privacy needs, as defined by the NIST Risk Management Framework (RMF) and its underlying publications and standards. In this role, we are responsible for providing the ISSO, system developers, system maintainers, and business owners security and privacy guidance to ensure NCHS systems are appropriately configured and maintained to meet the information security requirements outlined by A-123, FISMA, FedRAMP, HIPAA, HITECH, CIPSEA, as well as other applicable legislation, policies, guidance, and best practices established by OMB, NIST, HHS, or CDC. We provide support services in the areas of cybersecurity risk and compliance management, Security Assessment and Authorization (SA&A) audit analysis and support, software assurance, security awareness training, incident response, contingency planning, and policy implementation.					

10/06/2022 – IRS SPSS

Contract Name	Customer Name	Customer POC	Total Contract Value	Period of Performance	Is there a CPARS available, yes or no?
Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services to the National Center for Health Statistics (NCHS)	Centers for Disease Control & Prevention (CDC)	Avay Dolberry aym6@cdc.gov 919-541-2700	$1,585,531	7/3/2021 - 1/2/2026	Yes
Description of Services: RELI Group supports the NCHS ISSO in delivering information security services, guidance, and training to CDC information security stakeholders (e.g., business owners, security analysts, system developers, and other business partners), in the areas of cybersecurity risk and compliance management, Security Assessment and Authorization (SA&A) audit analysis and support, software assurance, security awareness training, incident response, contingency planning, and policy implementation.					
Contract Name	Customer Name	Customer POC	Total Contract Value	Period of Performance	Is there a CPARS available, yes or no?
Information Technology Cybersecurity	Indian Health Service (IHS)	David Causey david.causey@ihs.gov 301-443-0478	$21,440,541	8/15/2020 - 2/14/2026	Yes

Program Support Services (ITCPSS)					
Description of Services: RELI Group provides a full range of cybersecurity support services to IHS Division of Information Security (DIS), including cybersecurity program management and oversight, governance, risk and compliance support, Security Assessment & Authorization (SA&A) coordination, cyber threat analysis and incident response, security architecture and engineering, and disaster recovery and contingency planning.					

08/09/2022 – HHS OASH Cyber

Risk Management Framework (RMF)/ Cloud Security Operations Support Services [RELI – Prime]				
Contract Number	Dollar Value	Contract Type	Customer Name/Telephone	Role
75D30118C00588	$1,382,521.99	FFP/FUP	Avay Dolberry; 919-541-2700	Prime
Project Description: RELI provides cybersecurity consulting services to the Centers for Disease Control and Prevention (CDC) assisting the National Center for Health Statistics (NCHS) Information Systems Security Officer (ISSO) in meeting the cybersecurity and privacy needs. This includes SA&A work, authorization to operate (ATO) support, RMF support, policy and documentation support, security training and awareness support, GRC support and project management (PM) support.				

08/01/2022 - Department of Defense (DoD) / Defense Contract Management Agency (DCMA) - DCMA IT Cybersecurity Support Service (ITCSS)

Past Performance Reference # 3 [RELI]

Reference Number 3:	**Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services to the National Center for Health Statistics (NCHS)**
Name:	Avay Dolberry
Title:	COR
Agency, Address:	Centers for Disease Control and Prevention (CDC), 1600 Clifton Road Atlanta, GA 30329
Phone Number:	919-541-2700
E-Mail Address:	aym6@cdc.gov
Contract Title:	Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services to the National Center for Health Statistics (NCHS)
Contract No:/Type	75D30118C00588 / FFP/FUP
Contract POP:	04/03/18 - 07/02/21
Contract Value:	$1,382,521.99

Offerors are required to provide a brief description of the work performed under the referenced effort.

RELI provides cybersecurity consulting services to the Centers for Disease Control and Prevention's (CDC) National Center for Health Statistics (NCHS), assisting the NCHS Information Systems Security Officer (ISSO) in meeting the cybersecurity and privacy needs, as defined by the NIST Risk Management Framework (RMF) and its underlying publications and standards. In this role, we are responsible for providing the ISSO, system developers, system maintainers, and business owners security and privacy guidance to ensure NCHS systems are appropriately configured and maintained and meet the cybersecurity requirements outlined by A-123, FISMA, FedRAMP, HIPAA, HITECH, CIPSEA, as well as other applicable legislation, policies, guidance, and best practices established by OMB, NIST, HHS, and CDC.

Scope: RELI supports the Information Systems Security Officer (ISSO) in delivering security services and guidance to CDC business, security, and technical stewards. We do this in collaboration with Enterprise Performance Life Cycle (EPLC) coordinators, privacy personnel, other ISSOs, and the Office of the Chief Information System Officer (OCISO). We organize weekly meetings with NCHS ISSO, NCHS Confidentiality Officer, and EPLC representative, and provide the status of 14 NCHS IT projects' A&A and EPLC security milestones. We also created a NCHS Information Security SharePoint Site to share the cybersecurity and privacy guidance and training resources and references that we created for NCHS.

Magnitude: RELI supports the delivery of cybersecurity support in the areas of risk and compliance management, Assessment and Authorization (A&A) audit analysis and support, software assurance, security awareness training, incident response, contingency planning, and policy implementation.

Complexity: RELI provides RMF and A&A support to cybersecurity stakeholders (e.g., ISSO, business stewards, security stewards, Confidentiality Officer, business partners) in support of all of the security-related documentation and activities. Additionally, we provide interpretation of regulations, policy guidance, training material development/delivery, strategic support attaining/maintaining NCHS information systems security Authorization to Operate (ATO), risk analysis and guidance (e.g., system security requirements, weakness remediation, exception requests), and use of security tools (e.g., Trusted Agent, Tenable Security Center, WebInspect, Fortify).

Functional Area 1: Security Management

RELI provides contract management, including contract management plan development, dashboard reports, and program management support based on PMBOK, EPLC, CMMI, and ISO 9001. We facilitate weekly meetings with NCHS ISSO, NCHS Confidentiality Officer, and EPLC representative to provide the status of NCHS 14 IT projects' A&A and EPLC security milestones. RELI created the NCHS Information Security SharePoint Site to disseminate cybersecurity and privacy guidance and training resources that we developed for NCHS.

- RELI coordinates and manages meetings with relevant entities to ensure that time-sensitive and emerging issues are quickly identified and addressed, and to ensure that all deliverables are on-schedule. These meeting ensure that Risk-based discussions are ongoing and progressing towards acceptable resolutions within agreed-upon timeframes.

- RELI analyzes new and existing Federal, Department, and Agency mandates and guidance, as well as possible impacts of emerging technologies and solutions and assists NCHS in determining the most efficient, cost-effective way to implement them.
- RELI provides guidance to the NCHS ISSO, with regards to cybersecurity performance metrics, including the measurement of effectiveness of vulnerability remediation, security monitoring, and configuration management policy compliance.

RELI provides the NCHS ISSO with guidance in developing remediation plans to adequately address CDC-wide, A-123 and FISMA audit findings from agencies such as the U.S. Department of Homeland Security (DHS), Government Accountability Office (GAO), Office of Financial Management (OFM), and HHS. We also support the incident handling functions of reported NCHS security and privacy incidents, ensuring the appropriate incident triage, analysis, reporting, and response.

We perform risk assessments of information systems, business processes, and policy, and support vulnerability and weakness remediation, providing security steward guidance and facilitation with the Weakness Management Team.

Leveraging our subject matter expertise and CDC's software assurance and vulnerability management tools, RELI delivers risk analysis and compliance guidance of NCHS information systems' and IT projects' configurations, operating procedures, and corresponding documentation to ensure alignment with applicable regulations, policies, and standards.

RELI supports the incident handling functions of reported NCHS security and privacy incidents, ensuring the appropriate incident triage, analysis, reporting and response.

Functional Area 2: Security Engineering

RELI provides expert technical guidance to the NCHS ISSO and cybersecurity stakeholders to secure NCHS systems and IT projects in accordance with CDC security standards, HHS Enterprise Architecture (EA) standards, Enterprise Performance Life Cycle (EPLC) guidelines, and other applicable policies, procedures, and best practices. As part of this work, we perform the following services:

- Review system architecture designs, planned security controls, and proposed interconnection security agreements (ISA) to ensure appropriate configurations and controls are established for secure data management.
- Support and/or represents the NCHS ISSO on change control boards and associated work groups and committees to provide technical and operational support for issues such as vulnerability and patch management, configuration management, and other major configuration security related changes.
- Provide technical and management supervision and support for the CDM tools such as Trusted Agent, Archer, Tenable, and Fortify.
- Research and provide recommendations on security products, applications, protocols, systems, processes, new technologies, standards, guidelines, industry best practices, and other available information related to cybersecurity.

Functional Area 3: Security Compliance Group

RELI provides Risk Management Framework (RMF) compliance support and A&A training and guidance to security stakeholders (e.g., ISSO, business stewards, security stewards, Confidentiality Officer, business partners). We perform risk assessments of information systems, business processes, and policy, and support vulnerability and weakness remediation, providing security steward guidance and facilitation with the Weakness Management Team. RELI develops work products/tools, such as system security plan (SSP) templates with embedded instructions, risk assessment report templates, business process flow diagrams, and related documentation.

- RELI leverages our subject matter expertise and CDC's software assurance and vulnerability management tools to deliver risk analysis and compliance guidance of NCHS information systems' and IT projects' configurations, operating procedures, and corresponding documentation to ensure alignment with applicable regulations, policies, and standards.
- RELI developed and implemented a program to assist in the preparation of, tracking and reporting on FISMA compliance activities, including security authorization packages, annual security assessments, contingency plan tests, privacy impact assessments, and POA&M tracking. RELI organizes weekly meetings with NCHS ISSO, NCHS Confidentiality Officer, and EPLC representative, to provide the status of NCHS IT projects' A&A and EPLC security milestones, as well as the status of other security training tools, guidance, and related work products.

RELI evaluates A&A packages and related documentation providing analysis and guidance to system developers and maintainers regarding identified findings, architectural gaps, and policy/process deficiencies. We also assist in audit coordination, responding to requests for information from auditors, tracking weakness remediation process, and the resolution of POA&Ms by regular communication with system owners and system security personnel. We support the management and oversight of risk mitigation efforts to ensure acceptable resolutions are implemented within appropriate timeframes. Our services include performing analysis of all NCHS A&A documentation submitted for Annual Assessments and ATO pursual/renewal efforts, including Systems Security Plans (SSP), Privacy Impact Assessments (PIA), Business Continuity Plans (BCP), and other related system documentation.

05/09/2022 – Department of Defense (DoD) Defense Health Agency (DHA) Cybersecurity Technical Support Services

Customer	Contract Name	Contractor	Brief Description of Services
Centers for Disease Control & Prevention (CDC) National Center for Health Statistics (NCHS)	Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services	RELI Group	RELI supports the NCHS ISSO in delivering information security services, guidance, and training to CDC information security stakeholders (e.g., business owners, security analysts, system developers, and other business partners), in the areas of cybersecurity risk and compliance management, Security Assessment and Authorization (SA&A) audit analysis and support, software assurance, security awareness training, incident response, contingency planning, and policy implementation.

Relevance to Task 5.1.1 Cybersecurity Technical Support:

RELI provides expert technical guidance to the NCHS ISSO and information security stakeholders to secure NCHS systems and IT projects in accordance with CDC security standards, HHS Enterprise Architecture (EA) standards, Enterprise Performance Life Cycle (EPLC) guidelines, and other applicable policies, procedures, and best practices. As part of this work, we perform the following services:

- Review system architecture designs planned security controls, and proposed interconnection agreements to ensure appropriate configurations and controls are established for secure data management.
- Support and/or represents the NCHS ISSO on change control boards and associated work groups and committees to provide technical and operational support for issues such as vulnerability and patch management, configuration management, and other major configuration security related changes.
- Provide technical supervision and support for the CDM tools such as Trusted Agent, Archer, Tenable and Fortify.
- Research and provide recommendations on security products, applications, protocols, systems, processes, new technologies, standards, guidelines, industry best practices and other available information related to information security.

RELI also provides Risk Management Framework (RMF) and SA&A training and guidance to security stakeholders (e.g., ISSO, business stewards, security stewards, Confidentiality Officer, business partners). We perform risk assessments of information systems, business processes, and policy, and support vulnerability and weakness remediation, providing security steward guidance and facilitation with the Weakness Management Team.

Leveraging our subject matter expertise and CDC's software assurance and vulnerability management tools, RELI delivers risk analysis and compliance guidance of NCHS information systems' and IT projects' configurations, operating procedures, and corresponding documentation to ensure alignment with applicable regulations, policies, and standards.

RELI evaluates SA&A packages and related documentation (e.g., SSPs, PIAs, BCPs, etc.) providing analysis and guidance to system developers and maintainers regarding identified findings, architectural gaps, and policy/process deficiencies. We also assist in audit coordination, responding to requests for information from auditors, tracking weakness remediation process, and the resolution of POA&M by regular communication with system owners and system security personnel. Our services include performing analysis of all NCHS SA&A documentation submitted for Annual Assessments and ATO pursual/renewal efforts, including Systems Security Plans (SSP), Privacy Impact Assessments (PIA), Business Continuity Plans (BCP), and other related system documentation. We also provide remediation guidance for identified risks associated with assessment findings, architectural gaps, and policy/process deficiencies; and supports the management and oversight of risk mitigation efforts to ensure acceptable resolutions are implemented within appropriate timeframes.

RELI provides the NCHS ISSO with guidance in developing remediation plans to adequately address CDC-wide, A-123 and FISMA audit findings from agencies such as the U.S. Department of Homeland Security (DHS), Government Accountability Office (GAO), Office of Financial Management (OFM), and HHS. We also support the incident handling functions of reported NCHS security and privacy incidents, ensuring the appropriate incident triage, analysis, reporting and response.

Relevance to Task 5.1.2 Cybersecurity RMF Analyst:

RELI provides Risk Management Framework (RMF) and SA&A training and guidance to security stakeholders (e.g., ISSO, business stewards, security stewards, Confidentiality Officer, business partners). We perform risk assessments of information systems, business processes, and policy, and support vulnerability and weakness remediation, providing security steward guidance and facilitation with the Weakness Management Team. RELI develops work products/tools, such as system security plan (SSP) templates with embedded instructions, risk assessment report templates, business process flow diagrams, and related documentation.

RELI leverages our subject matter expertise and CDC's software assurance and vulnerability management tools to deliver risk analysis and compliance guidance of NCHS information systems' and IT projects' configurations, operating procedures, and corresponding documentation to ensure alignment with applicable regulations, policies, and standards.

RELI developed and implemented a program to assist in the preparation of, tracking and reporting on FISMA compliance activities, including security authorization packages, annual security assessments, contingency plan tests, privacy impact assessments, and POA&M tracking. RELI organizes weekly meetings with NCHS ISSO, NCHS Confidentiality Officer, and EPLC representative, to provide the status of NCHS IT projects' SA&A and EPLC security milestones, as well as the status of other security training tools, guidance, and related work products.

RELI evaluates SA&A packages and related documentation (e.g., SSPs, PIAs, BCPs, etc.) providing analysis and guidance to system developers and maintainers regarding identified findings, architectural gaps, and policy/process deficiencies.

04/08/2022 – IRS Bureau of Engraving and Printing (BEP) - Cybersecurity Support – Past Performance

Project Name: Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services		
A	Contract Number	Contract Number: 75D30121C11943
B	Contract Type	Fixed price with fixed unit price CLIN(s)
C	Government Agency/ Organization	Centers for Disease Control and Prevention (CDC) National Center for Health Statistics (NCHS)
D	Original Contract dollar value and final contract dollar value (including options)	Yearly Value: Base Period: $164,843.10; OY 1: $339,575; OY 2: $349,764.60; OY 3: $360,264.40; OY 4: $371,083.80 Total Value: $1,585,530.90
E	Original and final completion date	Start Date: 07/03/2021 End Date: 01/02/2026
F	**A description of the contract effort:** RELI supports the NCHS ISSO in delivering information security services, guidance, and training to CDC information security stakeholders (e.g., business owners, security analysts, system developers, and other business partners) in the areas of cybersecurity risk and compliance management, Security Assessment and Authorization (SA&A) audit	

	Project Name: Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services
	analysis and support, software assurance, security awareness training, incident response, contingency planning, and policy implementation.
G	**A brief narrative of why you deem the reference to be relevant to this effort:** RELI supports the ISSO in delivering security services and guidance to CDC business stewards, security stewards, and technical stewards. We do this in collaboration with Enterprise Performance Life Cycle (EPLC) coordinators, privacy personnel, other ISSOs, and the Office of the Chief Information System Officer (OCISO). We organize weekly meetings with the NCHS ISSO, NCHS Confidentiality Officer, and EPLC representative, and provide the status of 14 NCHS IT projects' SA&A and EPLC security milestones. We also created an NCHS Information Security SharePoint Site to share the information security and privacy guidance and training resources and references that we created for NCHS. **Task 1 – Security Assessment and Authorization:** RELI evaluates SA&A packages and related documentation, providing analysis and guidance to system developers and maintainers regarding identified findings, architectural gaps, and policy/process deficiencies. We also assist in audit coordination, responding to requests for information from auditors, tracking weakness remediation processes, and resolving Plans of Action & Milestones (POA&M) by regularly communicating with system owners and system security personnel. Our services include analyzing all NCHS SA&A documentation submitted for Annual Assessments and ATO pursual/renewal efforts, including System Security Plans (SSP), Privacy Impact Assessments (PIA), Business Continuity Plans (BCP), and related system documentation. We also provide remediation guidance for identified risks associated with assessment findings, architectural gaps, and policy/process deficiencies; and support management and oversight of risk mitigation efforts to ensure acceptable resolutions are implemented within appropriate timeframes. **Task 2 – Audit and Compliance:** RELI assists in coordinating audits, responding to requests for information from auditors, tracking weakness remediation processes, and resolving POA&Ms by regular communication with system owners and system security personnel. RELI provides the NCHS ISSO with guidance and information (data calls) in developing remediation plans to adequately address CDC-wide, A-123, and FISMA audit findings from such agencies as U.S. Department of Homeland Security (DHS), Government Accountability Office (GAO), Office of Financial Management (OFM), Office of Management and Budget (OMB), and HHS. **Task 3 – Information Systems Security Officer:** RELI is responsible for providing the NCHS ISSO security and privacy guidance to ensure NCHS systems are appropriately configured and maintained to meet the information security requirements outlined by A-123, FISMA, FedRAMP, HIPAA, HITECH, CIPSEA, and other applicable legislation, policies, guidance, and best practices established by OMB, NIST, HHS, or CDC. **Task 4 – Security Operations Center (SOC) and Cyber Engineering:** RELI supports the incident-handling functions of reported NCHS security and privacy incidents from the CDC

Project Name: Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services	
	SOC, ensuring appropriate incident triage, analysis, reporting, and response. RELI supports white papers on potential SOC operations and improvements. **Task 5 – Privacy Program:** RELI manages cybersecurity documentation and information maintained in CDC's Governance, Risk, and Compliance (GRC), including PIAs, PTAs, and SORNs. RELI performs cybersecurity and privacy research and prepares presentations and reports, as requested by the NCHS ISSO, to support advancement of the NCHS Risk Management Program. We also analyze federal and agency security and privacy requests for comments (RFC) and provide operational impact analyses and critical response on behalf of the NCHS ISSO. **Task 6 – Program and Project Management:** RELI manages the project, including developing a contract management plan, dashboard reports, and providing program management support based on PMBOK, EPLC, CMMI, and ISO 9001. As part of this work, we facilitate weekly meetings with the NCHS ISSO, NCHS Confidentiality Officer, and EPLC representative to provide the status of 14 IT projects' SA&A and EPLC security milestones. RELI created the NCHS Information Security SharePoint Site to disseminate information security and privacy guidance and training resources that we developed for NCHS. RELI also coordinates and manages meetings with relevant entities (e.g., business and system owners) to ensure that time-sensitive and emerging issues are quickly identified and addressed, and to ensure that all deliverables are on-schedule. These meetings ensure that risk-based discussions are ongoing and progressing toward acceptable resolutions within agreed-on timeframes. **Task 7 – Data Analytics:** RELI analyzes new and existing Federal, Department, and Agency mandates and guidance, as well as the potential impacts of emerging technologies and solutions and assists NCHS in determining the most efficient, cost-effective way to implement them. We also provide guidance to the NCHS ISSO, with regard to information security performance metrics, including the measurement of effectiveness of vulnerability remediation, security monitoring, and configuration management policy compliance. RELI analyzes all NCHS SA&A documentation submitted for Annual Assessments and ATO pursual/renewal efforts, including System Security Plans (SSP), Privacy Impact Assessments (PIA), Business Continuity Plans (BCP), and related system documentation. We provide remediation guidance for identified risks associated with assessment findings, architectural gaps, and policy/process deficiencies; and support management and oversight of risk mitigation efforts to ensure acceptable resolutions are implemented in appropriate timeframes. **Task 8 – Policy and Documentation:** RELI supports all security-related documentation and activities, including interpreting regulations and policy guidance, developing training materials, and providing strategic support to attain/maintain NCHS information systems' ATO. We also provide risk analysis and guidance, secure baseline configuration guidance, and security tool training and support. As part of our work, we perform cybersecurity and

Project Name: Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services		
	privacy research, and prepare presentations and reports for policy and documentation updates to support the NCHS Risk Management Program, as requested by the NCHS ISSO. We also analyze federal and agency security and privacy RFCs and provide operational impact analyses and critical responses (e.g., updated training guidelines) on behalf of the NCHS ISSO. **Task 9 – Cybersecurity Awareness Training Program:** RELI supports the NCHS ISSO in overseeing the delivery of information security awareness training and role-based security training to CDC information security stakeholders (e.g., business stewards, security stewards, technical stewards, developers, and other business partners) in the areas of risk and compliance management, SA&A audit analysis and support, software assurance, security awareness training, incident response, contingency planning, and policy implementation. **Task-10: Ad Hoc and Surge Requirements:** RELI's contract with CDC NCHS in all prior years included a surge support optional task that was always implemented and that RELI staffed and managed fully. **Transition In/Out:** RELI developed and implemented a Transition-In Plan that outlined a logical strategy to join the incumbent contract holder with RELI as the new prime contractor, while maintaining the incumbent contract holder as the new subcontractor, thus mitigating risk and loss of productivity to the government. Our collaborative, mission-oriented approach supported a smooth transition that saw no downtime or gaps in service. When a Transition Out Plan is required, we leverage that same collaborative and mission-oriented approach to ensure a smooth transition to our successor.	
H	COR's name, address, and phone number	Avay Dolberry, Contracting Officer's Representative aym6@cdc.gov 919-541-2700
I	Contracting Officer's name, address, and phone number	Tonya Justice, Contracting Officer wz01@cdc.gov 770-488-3282
J	Current status, e.g., completed and/or if in progress, start and estimated completion dates	In-progress. Start Date: 07/03/2021 End Date: 01/02/2026
K	Highlight key personnel who worked on the past performance referenced contract who are also	Not applicable.

<table>
<tr><th colspan="3">Project Name: Risk Management Framework (RMF) and Cloud Security Operations Support Consulting Services</th></tr>
<tr><td></td><td>being proposed for this effort</td><td></td></tr>
</table>