

STATE OF CALIFORNIA
Budget Change Proposal - Cover Sheet
 DF-46 (REV 08/15)

Fiscal Year 2016-17	Business Unit 8940	Department California Military Department	Priority No. 1
Budget Request Name 8940-001-BCP-BR-2016-GB		Program 6911 National Guard	Subprogram 6911035 Military Civil Support

Budget Request Description
 Cyber Network Defense Team

Budget Request Summary

The California Military Department requests position and reimbursement authority for the Department's **Cyber Network Defense Team** (CNDT).

Requires Legislation <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Code Section(s) to be Added/Amended/Repealed	
Does this BCP contain information technology (IT) components? <input type="checkbox"/> Yes <input type="checkbox"/> No <i>If yes, departmental Chief Information Officer must sign.</i>	Department CIO	Date
For IT requests, specify the date a Special Project Report (SPR) or Feasibility Study Report (FSR) was approved by the Department of Technology, or previously by the Department of Finance. <input type="checkbox"/> FSR <input type="checkbox"/> SPR Project No. Date:		

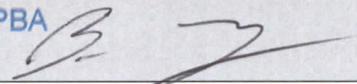
If proposal affects another department, does other department concur with proposal? Yes No
Attach comments of affected department, signed and dated by the department director or designee.

Prepared By LTC James Parsons 	Date 2 Sep 15	Reviewed By COL (CA) Darrin Bender 	Date 2 Sep 15
Department Director COL Robert Spano 	Date 2 Sep 15	Agency Secretary	Date

Department of Finance Use Only

Additional Review: Capital Outlay ITCU FSCU OSAE CALSTARS Dept. of Technology

BCP Type: Policy Workload Budget per Government Code 13308.05

PPBA 	Date submitted to the Legislature 11/7/16
---	--

BCP Fiscal Detail Sheet

BCP Title: Cyber Network Defense Team

DP Name: 8940-001-BCP-DP-2016-GI

Budget Request Summary

	FY16					
	CY	BY	BY+1	BY+2	BY+3	BY+4
Positions - Permanent	0.0	2.0	2.0	2.0	2.0	2.0
Total Positions	0.0	2.0	2.0	2.0	2.0	2.0
Salaries and Wages						
Earnings - Permanent	0	226	226	226	226	22
Total Salaries and Wages	\$0	\$226	\$226	\$226	\$226	\$22
Total Staff Benefits	0	121	121	121	121	12
Total Personal Services	\$0	\$347	\$347	\$347	\$347	\$34
Operating Expenses and Equipment						
5320 - Travel: In-State	0	95	95	95	95	9
5346 - Information Technology	0	140	140	140	140	14
Total Operating Expenses and Equipment	\$0	\$235	\$235	\$235	\$235	\$23
Total Budget Request	\$0	\$582	\$582	\$582	\$582	\$58

Fund Summary

Fund Source - State Operations						
0001 - General Fund	0	0	0	0	0	
0995 - Reimbursements	0	582	582	582	582	58
Total State Operations Expenditures	\$0	\$582	\$582	\$582	\$582	\$58
Total All Funds	\$0	\$582	\$582	\$582	\$582	\$58

Program Summary

Program Funding						
6911035 - Military Civil Support	0	582	582	582	582	58
Total All Programs	\$0	\$582	\$582	\$582	\$582	\$58

Personal Services Details

		Salary Information								
		Min	Mid	Max	<u>CY</u>	<u>BY</u>	<u>BY+1</u>	<u>BY+2</u>	<u>BY+3</u>	<u>BY+4</u>
Positions										
	1387 - Dp Mgr IV (Eff. 07-01-2016)				0.0	1.0	1.0	1.0	1.0	1.0
	8366 - W4 (Eff. 07-01-2016)				0.0	1.0	1.0	1.0	1.0	1.0
Total Positions					0.0	2.0	2.0	2.0	2.0	2.0
		CY	BY	BY+1	BY+2	BY+3	BY+4			
Salaries and Wages										
	1387 - Dp Mgr IV (Eff. 07-01-2016)	0	108	108	108	108	10			
	8366 - W4 (Eff. 07-01-2016)	0	118	118	118	118	11			
Total Salaries and Wages		\$0	\$226	\$226	\$226	\$226	\$226	\$22		
Staff Benefits										
	5150350 - Health Insurance	0	42	42	42	42	4			
	5150500 - OASDI	0	20	20	20	20	2			
	5150600 - Retirement - General	0	55	55	55	55	5			
	5150800 - Workers' Compensation	0	4	4	4	4				
Total Staff Benefits		\$0	\$121	\$121	\$121	\$121	\$121	\$12		
Total Personal Services		\$0	\$347	\$347	\$347	\$347	\$347	\$34		

Analysis of Problem

A. Budget Request Summary

The California Military Department requests an increase in reimbursement authority from \$774,000 to \$1,356,000 to pay for eight permanent positions (six existing positions and two new permanent positions) for the Department's *Cyber Network Defense Team* (CNDT). The funding will also pay for hardware and software needed by the CNDT to conduct cyber security assessments for 35 state agencies per year. The CNDT would also be able to simultaneously respond to 4 cyber-incidents per year to mitigate loss of data, restore network services, and assist law enforcement.

B. Background/History

The CNDT began as a pilot program in 2013 with a proof of concept grant from the Speaker of the Assembly. In FY 2014-15, six permanent positions were approved via the Budget Act of 2014. The CNDT leverages military cyber security training and equipment to provide state-of-the-art assistance and expertise to state agencies before, during, and after a cyber-attack.

AB 670 (Irwin) amended section 11549.3 of the Government Code to require the Chief Information Officer to ensure that at least 35 state agencies per year receive independent cyber vulnerability assessments. The CNDT is the only capability within state government capable of conducting these mandated assessments.

The CNDT provides support services which include: Network Health Assessments, Agency Vulnerability Assessments, Continuous Network Monitoring, Firewall Analysis, Website Vulnerability Scans, Network Infrastructure Endpoint Discovery and Identification, Network Traffic Anomaly and Indicators of Compromise, and Endpoint Malware Binary and Indicators of Compromised Binary Discovery services. In addition to these current services, the CNDT is preparing to offer Penetration Testing and Computer Forensics support.

Resource History
(Dollars in thousands)

Program Budget	PY - 4	PY - 3	PY - 2	PY - 1	PY
Authorized Expenditures	0	0	0	510	884
Actual Expenditures	0	0	0	509	344
Revenues	0	0	0	0	0
Authorized Positions	0	0	0	0	6
Filled Positions	0	0	0	0	4
Vacancies	0	0	0	0	2

Workload History

Workload Measure	PY - 2	PY - 1	PY	CY
Cyber Security Assessments and risk mitigation consultations	30	35	15	5
Cyber Incident Response				3

C. State Level Considerations

According to State Administrative Manual (SAM) 5330.1, State of California organizations using computer networks are required to "perform security assessments to determine whether the security controls selected by the state entity are implemented correctly and working as intended to mitigate risk". The SAM also requires each agency to have an independent (external) vulnerability assessment of their network every other year. In other words, the state requires that approximately 80 external cyber vulnerability assessments be conducted on state agencies networks every year.

External assessments required by the SAM are not being done. However, the CNDT has found that if conducted, these external vulnerability assessments are very effective in reducing network vulnerabilities. In fact, as of January 2015 the CNDT had discovered and provided remediation plans for over 659,000 vulnerabilities on state computer systems and networks, greatly reducing the risk of successful attack/penetration of those networks and systems.

Analysis of Problem

The CNDT also continuously interviews state Information Security Officers and Chief Information Officers to identify critical capability shortfalls and develop new services, further enhancing the value the team adds to California.

D. Justification

Cybercrime is a dangerous and growing threat to the State of California. The cost of repairing compromised networks is vastly higher than investing to prevent a cyber-attack. In June of this year, government cyber-attacks comprised over 20% of all reported cyber-attacks. Recent examples of information breaches like that of the Federal Office of Personnel Management (22 million personnel records compromised) highlight the need for the State of California to increase vigilance against cyber-attacks against the state network.

According to the California Information Security Office (CISO), between the periods of January to June 2015, there have been over 1,500 reported cyber-related incidents involving California systems. It is important to note these were detected and reported attacks; typically a much larger number of attacks occur and remain undetected.

In 2014-15, the CNDT found 33.84 possible means of intrusion per computer system on the state networks based on a sample size of almost 15,000 systems. By comparison, the Department of Defense considers any computer with more than four vulnerabilities to be compromised and immediately removes it from the network.

A 2013 study by the Ponemon Institute found that the cost of network attacks rose nearly 20% per year. In addition to mounting costs, the study demonstrated that the prevention of an attack by network hardening can greatly reduce the cost of an attack. According to the study, the mean number of days needed for an organization to resolve a cyber-attack was 32 days, with an average cost per day of \$32,469 for a total remediation cost of \$1,035,769. That cost rose from 2012 to 2013 at a rate of 55%. The CNDT has the ability to reduce the risk of an attack. In the event of an attack, the CNDT, under the authority of OES, can quickly respond to the victimized agency and assist law enforcement to find and prosecute those responsible.

The Department of Technology reported that cyber incidents in state government cost the state over \$2.5 million dollars in 2011-2012.

To protect the state's information assets from a wide spectrum of threats and risks, state organizations are required to implement general controls, including information security and privacy policies, standards, and procedures specified in Chapter 5300 of SAM. A 2013 review by the Department of Technology of compliance of the self-certification process concluded that only 112 of 140 (80 percent) have self-certified compliance to their Risk Management and Privacy Program Compliance (SIMM 70C); less than 60 percent have certified full compliance with information security policy directives, and less than 70 percent have indicated a risk assessment has been performed within the past two years.

According to the Department of Technology "self-certification without independent validation does not ensure compliance or effective risk management." The Department of Technology's auditing program only has the capacity to assess the network compliance of a handful of state agencies per year (if that). With over 200 state agencies and entities, the scale of the Department of Technology's audit program is too small to address the cyber security vulnerability of the state network. Comparatively, the CNDT can assess over 40 agencies per year; a much more appropriate capability given the amount of work that must be done to reduce the high risk, and high cost, of a cyber-attack.

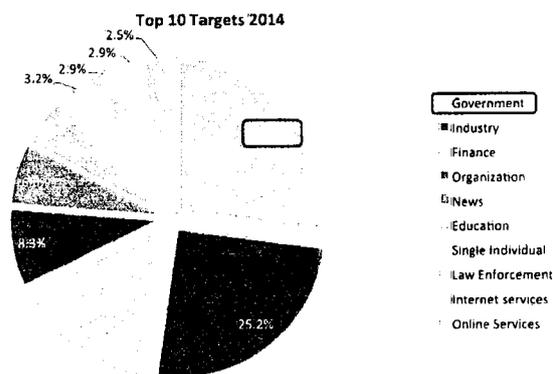
Counting on state agencies to "self-assess" doesn't work. According to the Department of Technology, many state entities either:

- Do not certify some, or all, of the requirements in the State Information Management Manual; or
- They certify compliance without actually completing the required Information Technology (IT) security tasks.

Analysis of Problem

The Department of Technology acknowledges that it does not have the resources necessary to follow up with non-certifiers or verify actual compliance of required external certifications. Therefore the State must accept a significant amount of IT security risk. The CNDT is a proven capability that can significantly reduce IT security risk to the state very efficiently and cost effectively.

The services that the CNDT delivers are unique, found nowhere else in state government. The CNDT has a proven track record of providing the core services and expertise desperately needed by agencies to identify and reduce their overall risk related to state network compromise. The expertise the CNDT provides to agencies allows the State to recognize significant cost avoidance when compared to contracted services and provides a ready response capability in the event of network compromise.



Statistically the Top target category attacked in 2014 was Government

The CNDT uses federal cyber security training (paid for by the Department of Defense) and military cyber expertise and best business practices to assist state agencies by assessing the strengths and vulnerabilities of their networks and providing actionable recommendations, assistance, and services designed to improve overall cyber security compliance. In addition to its prevention efforts, the CNDT is uniquely positioned within the state to provide reach back support to state agencies through its access to classified federal cyber intrusion information. Due to the highly classified nature of cyber and the level of clearance its members hold, the CNDT can provide directed

Incident Response assistance to impacted agencies that would otherwise not be available. The CNDT has demonstrated its rapid response capability on multiple occasions in 2014-15 and 2015-16, responding in hours of the request for assistance while preserving the agency confidentiality.

The CNDT will consist of eight full-time staff and eight traditional Guard members (part-time) with a focus of Defensive Cyber Operations. The mission of this group is to reduce risks to government computer networks and react to cyber-attacks that occur anywhere in the state as tasked by the Governor's Office of Emergency Services (OES). The CNDT retains links to both state and local government as well as federal agencies such as the Federal Bureau of Investigation, Department of Homeland Security, and other federal entities. Members of the CNDT retain certifications in a wide variety of core commercially recognized cybersecurity competencies in addition to obtaining high level security clearances that should satisfy the standards of the most stringent regulatory bodies.

The CNDT also participates in several annual national cyber defense exercises including *Cybershield* and *CyberGuard*. Members of the CNDT support the local community through participation in educational and mentorship opportunities in cyber, such as the San Diego *Securing Our E-city Foundation Cyber Boot Camp* and *Cyberpatriot*, which provides instruction to middle and high school students.

E. Outcomes and Accountability

Approval of this proposal will allow the CNDT to continue to effectively harden California government networks from cyber-attack. If approved, the CNDT would coordinate with OES and Department of Technology to prioritize agencies and provide 35 assessments per year. If necessary, the CNDT could surge to a staff of 16 cyber security experts to immediately respond to a cyber-incident anywhere within the state.

The CNDT will continue to track vulnerability reductions within the state and will maintain information related to amount and types of risks removed and/or reduced. The CNDT will account for all support provided and will continue to safeguard the sensitive information discovered with supported entities.

Analysis of Problem

Projected Outcomes

Workload Measure	CY	BY	BY+1	BY+2	BY+3	BY+4
Cyber Security Vulnerability Assessment and Risk Mitigation Consultation	10	35	35	35	35	35
Cyber Incident Responses	3	4	4	4	4	4

F. Analysis of All Feasible Alternatives

Alternative 1: Increase reimbursement authority from \$774,000 to \$1,356,000 per year to provide 35 cyber security assessments to state agencies. The Department will be reimbursed thru the Department of Technology in accordance with an existing Memorandum of Agreement.

Pros:

- Uses existing cyber security specialists that are trained and ready right now to reduce the risk of devastating cyber-attack(s) on the state network that could cost tens of millions of dollars and put California's citizens' private information at risk.
- Allows the state to target assessments to those agencies that are higher priority (house more sensitive personal data, etc.).
- Maintains relationships with state and federal agencies to enhance communication and cyber threat information sharing.
- Conducts cyber-security assessments and risk reduction consultation for 35 state agencies per year.
- Promotes interagency coordination and cooperation.
- Creates a baseline assessment process (developed in coordination with the Department of Technology) that is in-line with state requirements and best business practices.
- Represents the best value for the state at a fraction of the cost of a private sector vendor.
- Ensures compliance with the requirement in AB 670 that the state conduct 35 independent security assessments per year.
- Gives the state the authority to modify/evolve the cyber assessment process in a seamless and uniform manner by using single source to implement changes.
- Provides Department of Technology and the OES with tasking authority of the CNDT, ensuring that agencies are assessed in priority order and in accordance with the information security risk index.
- Provides for a single source to collect and share all data and analysis that results from the 35 mandated assessments per year.
- Provides for better security of assessment data by creating a single collection point.
- Uses cyber security specialists whose state-of-the-art training is funded by the Department of Defense.
- Leverages existing relationships with state and federal agencies (CHP, Department of Justice, U.S. Cyber Command, FBI, U.S. Department of Homeland Security) to enhance cyber threat information sharing.
- Establishes a 24/7 Cyber Incident Response capability for the state that can deploy at a moment's notice and mitigate damage and data loss anywhere in the state.
- Incentivizes state agencies to strengthen their network security by providing network vulnerability assessments and risk reduction consultation.

Analysis of Problem

NOTE: The CNDT has received overwhelmingly positive feedback from agencies that their consultation services have allowed the assessed agency to adopt procedures that significantly reduced cyber security risks.

- Provides the state access to a significant amount of aggregated data regarding the health of the state network, vulnerability trends, and best business practices. This information can be used to establish policy and effectively direct resources to target common vulnerabilities or problem areas.

Cons:

- Expands state government by increasing existing program from six to eight members.
- Requires state agencies to pay for cyber security assessments with money that could be used to by new IT equipment or software.
- Would only allow the CNDT to assess every state agency approximately once every five years; far below the SAM requirement that every agency be assessed once every two years.

Alternative 2: Continue fee for service based support:

Pros:

- No increase in state government.
- Would only cost those agencies that volunteer for assessments.
- Approximately 20 agencies per year could receive vulnerability assessments.

Cons:

- Does not significantly increase information security of state government data.
- Does not allow for an effective way to comply with the requirement of AB 670 that 35 agencies be assessed each year
- Does nothing to move toward the SAM requirement that approximately 80 agencies per year be assessed.
- With a fee for service model, the California Military Department must assume all financial risk of revenue not covering costs. This puts the continued viability of the CNDT at risk.
- The CNDT is not funded to provide 24/7 cyber incident response.

G. Implementation Plan

Upon approval, the CNDT will coordinate with OES and the Department of Technology to assess prioritized agencies. The CNDT will be immediately available to respond to a cyber-emergency when tasked by OES. The method of receiving payment from assessed agencies will remain the same as it is currently.

H. Supplemental Information

None.

I. Recommendation

Approve alternative 1 as proposed. Invest in a permanent strategy to reduce computer network risk within the state and provide the ability to rapidly react to possible network breaches in order to minimize the severity of the attack.

CYBER NETWORK DEFENSE TEAM
 WORKLOAD ANALYSIS FOR
 CND
Senior Cyber Security Engineer (CW4)

Performs under the direct supervision of the CND Team OIC. Responsible for the training of all Cyber Analysis and supervisors in matters related to technical tool application, deployment, best practice usage, data collection, analysis, and archival. Responsible for supervising the analysis of multiple agency host security vulnerabilities and configurations with regards to industry standard compliance guidelines including but not limited to NIST, ISO27001, PCI, and FERC. Acts as the direct supervisor for Team Cyber Analyst Team Leaders. Manages the technical aspects related to identification, collection, and analysis of Incident Response artifacts. Performs initial technical analysis of all cyber analyst generated customer findings related to vulnerability management, firewall compliance, system hardening, and website analysis. Provides assist to the Agency penetration testing team in matters related to scanning, vulnerability identification, and documentation. Performs maintenance of cyber analysis backend servers, collection systems, and other devices.

TASKS

Technical Cyber Product Analysis (50)	1128 Hours
--	-------------------

- a) Ensures cybersecurity analysis results are consistent with industry established Best Business Practices, Compliance Standards, and Customer requirements (3 hrs Weekly / 156 Hrs Annually)
- b) Performs initial technical analysis of all cyber analyst generated customer findings related cybersecurity services rendered (8 hrs Weekly / 416 Hrs Annually)
- c) Manages the technical aspects related to identification, collection, and analysis of Incident Response artifacts (100 hrs Annually)
- d) Develops training curriculum for all current Cyber Analysis Tools (30 hrs Monthly / 360 Hrs Annually)
- e) Reviews and manages all tool SOP's and related internal publications (8 hrs Monthly / 96 Hrs Annually)

System Administration and Maintenance (25)	756 Hours
---	------------------

- a) Brief CND Manager on current system status, lifecycle operations, and disaster recovery testing results (1 hr Weekly / 52 Hrs Annually)
- b) Manages air-gaped secure storage and destruction procedures (2 hrs Weekly / 104 Hrs Annually)
- c) Performance vulnerability management of CND systems, servers, and network hardware
- d) Perform cybersecurity tool upgrades (8 hrs Weekly / 416 Hrs Annually)
- e) Perform Disaster Recovery and testing operations for CND systems (12 hrs Monthly / 144 Hrs Annually)
- f) Order repair parts, license renewals, and version upgrades for CND tools and devices (40 hrs Annually)

Management, Supervision, Information Sharing, and Support (25)**532 Hours**

- a) Resolves manpower and availability related issues with Resource Coordinator regarding multi-agency team lines of effort including team and tool availability (3 hrs Monthly / 36 Hrs Annually)
- b) Supervises all Cyber Analysis Team Leaders (3 hrs Weekly / 156 Hrs Annually)
- c) Provides assist to the Agency penetration testing team in matters related to scanning, vulnerability identification, and documentation (40 hrs Annually)
- d) Prepared briefings for Agency and External entities related to anonymized findings, cyber Incident Responses, and other support missions (18 hrs Monthly / 216 Hrs Annually)
- e) Act as team Point of Contact for all deployment reporting requirements (24 hrs Annually)
- f) Acts as primary coordinator for intra-organization cyber events and exercises (60 hrs Annually)

Total Hours per Year: 2,416

CYBER NETWORK DEFENSE TEAM
WORKLOAD ANALYSIS FOR
CND
Cyber Operations Manager (DPM IV)

Performs at the Subject Matter Expert (SME) level regarding matters related to Cybersecurity, Incident Response, Penetration Testing, Information System Malware Defense, Vulnerability Mitigation, and network perimeter defense including intrusion detection and prevention systems. Acts independently on multiple projects and lines of effort regarding the cybersecurity and defense of multiple State Customer networks and security enclaves. Responsible for providing high-level expertise and advice to executive-level staffs including external Agency Directors, Chief Information Officers, and Information Security Officers. Maintains appropriate and relevant educational awareness and training related to ongoing technology trends, risks, and technologies relevant to a broad spectrum of state agency current and future deployed technologies. Supervises agency Incident Response teams, Cybersecurity Analysts, and other technical support staff. Provides Serves as the Alternate Shift Network Operations and Security Center (NOSC) manager, supporting multiple shifts (as required) and during crisis response periods. Responsible to develop analysis, Tactics, Techniques, and Procedures (TTPs), and evaluate existing processes related to the relevance, requirements, and delivery of multi-agency cybersecurity support services. Performs state policy and depending legislative analysis regarding cyber impacts to agency and support entities. Facilitates external relationships with multiple Federal, State, Local, Tribal, and Territorial entities for matter related to Multi-Agency relationship regarding Cybersecurity and Incident Response. Reviews departmental requirements related to current computer industry technology, including the practices on data security, integrity, availability, audit compliance, product evaluation, installation, maintenance, and control of information systems software. Possesses the knowledge, skills, abilities and background clearances to successfully operation within different network sensitivity levels including public, sensitive, and government restricted (including classified network segments).

TASKS

Cyber Defensive Process and Tactics Development	892 Hours
a) Reviews and performs gap analysis of agency Tactics, Techniques, and Procedures (TTPs) related to Incident Response (24 hrs Month / 288 Hrs Annually)	
b) Develops technical analysis for internal and external agency provided Penetration Testing (60 hrs Quarter / 240 Hrs Annually)	
c) Performs technical analysis of tools, processes, and products related to multiple external agency vulnerability and perimeter defense assessments (8 hrs Monthly / 96 Hrs Annually)	
d) Reviews existing anti-malware defensive and vulnerability management posture to provide Executive-level analysis and recommendations (4 hrs Weekly / 208 Hrs Annually)	
e) Possesses and maintain background clearances to successfully operation within different network sensitivity levels including public, sensitive, and government restricted networks including classified network segments (60 hrs Annually)	

Technical Product Development and Review**564 Hours**

- a) Performs Subject Matter Expert level cybersecurity analysis, technical direction, and analyst support for live and static collected cybersecurity artifacts / indicators from multiple State Customer networks and security enclaves to (7 hrs Weekly / 364 Hrs Annually)
- b) Develops analysis, Tactics, Techniques, and Procedures (TTPs), and existing processes review of multi-agency cybersecurity support services (10 hrs Month / 120 hrs Annually)
- c) Reviews Agency requirements related to current computer industry technology, including the practices on data security, integrity, availability, audit compliance, product evaluation, installation, maintenance, and control of information systems software (80 hrs Annually)

Staff Management**419 Hours**

- a) Supervises agency Incident Response teams (15 hrs Annually)
- b) Supervises Cybersecurity Analysts (5 hrs Weekly / 260 Hrs Annually)
- c) Supervises other permanently and temporarily assigned technical support staff
- d) (1 hr Week / 52 Hrs Annually)
- e) Supervises Network Operations and Security Center (NOSC) alternate shift and during crisis response periods (40 Hrs Annually)
- f) Provides Information Assurance (IA) and Cybersecurity Compliance oversight to Agency operations (1 hrs Weekly / 52 Hrs Annually)

Internal / External Staff / Executive Interaction**320 Hours**

- a) Provides Agency Director and other Senior Staff members subject matter expertise for issues regarding Cybersecurity (2 hrs Weekly / 104 Hrs Annually)
- b) Provides Subject Matter Expert level analysis to external state agencies and other mission partner activates regarding Cyber Defense, Cyber Security, and Incident Response (9 hrs Monthly / 108 Hrs Annually)
- c) Provides briefings, reports, and analysis to external Agency Directors, Chief Information Officers, and Information Security Officers (5 hrs Monthly / 60 Hrs Annually)
- d) Facilitates external relationships with multiple Federal, State, Local, Tribal, and Territorial entities for matter related to Multi-Agency relationship regarding Cybersecurity and Incident Response (4 hrs Monthly / 48 Hrs Annually)

Information Sharing and Coordination (5)**270 Hours**

- a) Identifies, analyzes, and prepares internal products related to the adoption of new and existing state technology trends and risks (7.5 hrs Monthly / 90 Hrs Annually)
- b) Coordinate with Chief Information Security Office and State Threat Assessment Center on matters related to cybersecurity risks and mitigations (3 hrs Monthly / 36 Hrs Annually)
- c) Participate in cybersecurity related councils, working groups, task forces, and committees (12 hrs Monthly / 144 Hrs Annually)

Policy Analysis and Advisory Functions

108 Hours

- a) Performs Agency analysis and develops internal products related to cybersecurity policy and process impacts (5 hrs Monthly / 60 Hrs Annually)
- b) Performs legislative analysis and develops internal products regarding cyber impacts to agency and support entities (4 hrs Weekly / 48 Hrs Annually)

Total Hours per Year: 2,573