|  |  |  |  |
| --- | --- | --- | --- |
| ICS OT IoT Security Risk Assessment  Scope and Statement of Work | | |  |
| Date | Services Performed By: | Services Performed For: | |
| [Date] | [Company Name]  [Company Address] [City, ST ZIP Code] | Customer  Customer Address | |

|  |  |  |
| --- | --- | --- |
|  |  |  |

# ICS OT IoT Security Assessment Approach

The purpose of an ICS OT IoT focused security risk assessment is to focus on operational mission and business resilience. Resilience ensures that when an organization is under attack, particularly when their ICS OT IoT assets have been modified, sabotaged or failed that the organization can continue to operate in a degraded state as well as that the interdependent surrounding environment, community, customers and supply chain of the asset owners is less impacted by the consequences of successful threat events against ICS OT IoT assets and operations. This perspective provides a comprehensive, actionable and mission operations focused approach to a security risk assessment. It is specifically designed for ICS OT IoT asset owners and operators especially for owners and operators with consequences and impacts that could cause harm to the environment or threaten human life, health, and safety.

# Overview of Consultant

Consultant is focused on providing ICS OT IoT focused security consulting services. Consultant brings national security, critical infrastructure, information assurance, information security, and mission assurance global experiences to all ICS OT IoT security risk assessments. In addition to assessments Consultant provides a variety of other ICS OT IoT security focused services that cover strategic, tactical, and operational levels of the lifecycle of an ICS OT IoT asset and the asset owner’s operations.

# Scope of Work

The scope of work defines the key milestones, phases, tactics, techniques, tools, and deliverables involved in the ICS OT IoT security risk assessment.

* **Open Source Intelligence & Public Facing Vulnerability Analysis**

This is used to determine how open the public footprint of the customer is and gather information that attackers would have leverage of to further target the customer.

* **Business Mission Purpose and Objectives**

This is used to interview key positions throughout different business units and discipline areas of the organization to determine the purpose of the business, it is most critical locations and product lines and its crown jewels. This is also used to determine its environment, sector, regulatory requirements, customers etc.

* **Supply Chain, Third Party, Governance, Maturity level & Standards Gap Assessment**

This is used to gather information about security governance and maturity levels for ICS OT IoT as well as gain an understanding of and access to the ICS OT IoT and organizational supply chain as well as third parties with impact to ICS OT IoT.

* **Technical Vulnerability Assessment**

This is used to both passively and actively discover vulnerabilities within networks, applications, assets, and systems that directly impact the ICS OT IoT operations and the environment.

* **Physical Tour Boots on the Ground Assessments**

This is used to gain eyes on the ICS OT IoT assets and critical operations on the ground at critical sites. It is necessary in ICS OT IoT and the primary difference between an ICS OT IoT security risk assessment and a traditional IT corporate risk assessment. Going into the field operations separates assumptions and outdated documentation from reality.

* **Threat, Consequence, Impact, Vulnerability, Interdependency, Risk Analysis**

This is used to analyze all gathered information about the organization and its ICS OT IoT operations and assets. This is where that information is used to map ICS OT IoT assets, people, processes and technologies to vulnerabilities, threats, consequences, and impacts.

* **Recommendations**

This is used to break out discovered risks into actionable and mitigative risk, consequence and impact reduction tasks that can counter threats and vulnerabilities.

* **Optional Red Team Penetration Test (additional cost and scope with separate rules of engagement)**

This is an optional addition to the ICS OT IoT security assessment. Red Team penetration tests are used in addition to all other phases of an ICS OT IoT security risk assessment specifically to attempt to exploit discovered vulnerabilities in people, processes, and technologies. Red team pentests are specifically helpful in further testing advanced offensive attacks against ICS OT IoT assets and adjacent systems that impact ICS OT IoT to determine which threats and vulnerabilities are easier to exploit than others and which are harder to exploit. This enables the asset owner to further fine tune recommendations and further prioritize ICS OT IoT assets, consequences, impacts, threats, and vulnerabilities.

# Delivery Period

Describe the delivery agreements between the consultant and customer.

# Project Management & Communication

The project shall begin with a “kick-off” meeting where the teams are introduced and expectations, schedules, rules of engagement, and other procedures are discussed. Consultant will work with customer points of contact on a weekly basis where applicable as well as before and after site visits to provide updates on progress of the assessment tasks and phases. Communication will occur primarily through email, phone call and conference meeting invites set up by consultant.

# Methodology and Approach

As defined in scope of work the ICS OT IoT security risk assessment scope of work section. Below goes into a bit more details about what a customer should expect in each phase and task including examples of tools used, expected deliverables and requirements from customers for the assessment to be successful and meaningful. Please note that the list of tools are an example and will always be customized based on the environment and scope of targets etcetera. The list of tools will be determined by the consultant. The consultant will make the customer aware of any tool changes before, during and after the assessment engagement.

## Open Source Intelligence & Public Facing Vulnerability Analysis

This is used to determine how open the public footprint of the customer is and gather information that attackers would have leverage of to further target the customer. Some of the tools here used during the assessment are also used during the reconnaissance phase of red team penetration tests.

### Example Tools & References

* SearchDiggity
* Nmap
* Google
* SHODAN
* The Harvester
* Wikimapia
* OpenStreetMap
* Job posting sites (e.g., Glassdoor, LinkedIn, Indeed etc.)
* Government regulatory sites (search case filings from SEC, FCC, FDA, FERC, local utility commissions etc.)
* RECON-NG
* Whois
* Maltego
* Nessus

### Required deliverables from Customer

* Public facing IPs and domains
* List of known third parties
* Names of business units and locations of selected critical sites in scope of assessment

### Consultant Deliverables

* Capture of public facing vulnerabilities
* Capture of potential pivot and targeting information
* Screen shots and narratives of findings
* Recommendations for reducing vulnerabilities
* Identification and notification of any discovered threats

## Business Mission Purpose and Objectives

This is used to interview key positions throughout different business units and discipline areas of the organization to determine the purpose of the business, it is most critical locations and product lines and its crown jewels. This is also used to determine its environment, sector, regulatory requirements, customers etc. During these interviews and documentation reviews you assess the risk tolerance of the organization, security maturity levels and where its crown jewels could be. This is also where you begin to rank, classify and categorize business units, systems, and assets. This enables you to take an all hazards and all threats view of strategic, tactical, and operational impacts to the organization and ICS OT IoT assets and operations.

### Example Tools & References

* DHS CSET
* AEM Corps “PARRE” tool
* DOE C2M2
* NIST Cybersecurity Framework
* Exida’s CyberPHAx tool
* Bowtie
* Crown Jewels Analysis
* Mission Assurance Dependency Analysis
* Asset, Mission, Site, Product, Region value classifications

### Required deliverables from Customer

* Access to requested personnel, documents, sites, third parties and assets

### Consultant Deliverables

* Risk categorization of business units, crown jewel ICS OT IoT assets, and operations identification
* Risk scoring of business units and in scope sites and related ICS OT IoT assets and operations
* Determination of people, process, and technology maturity levels with impact to ICS OT IoT assets and operations
* Understanding of all hazards and all threats consequences and impacts to organization and ICS OT IoT assets and operations such as financial costs, environmental, human life, and safety etcetera.

## Supply Chain, Third Party, Governance, Maturity level & Standards Gap Assessment

This is used to gather information about security governance and maturity levels for ICS OT IoT as well as gain an understanding of and access to the ICS OT IoT and organizational supply chain as well as third parties with impact to ICS OT IoT.

### Example Tools & References

* NIST SP 800-161, 160, 171 etc.
* DHS CSET
* DOE C2M2
* Customer information on contracts, suppliers, third party access, agreements etc.
* Open Source Intelligence tools
* Merger, Acquisition and Divestment information
* Procurement information (e.g., public tender/RFP/RFI details, etc.)
* Service Level Agreements, Master Services Agreements etc.

### Required deliverables from Customer

* Access to requested personnel, documents, sites, third parties and assets

### Consultant Deliverables

* Understanding of supply chain and third-party risks to ICS OT IoT and operations
* Understanding of vulnerabilities in governance, policies, procedures, roles, responsibilities, and contract agreements

## Technical Vulnerability Assessment

This is used to both passively and actively discover vulnerabilities within networks, applications, assets, and systems that directly impact the ICS OT IoT operations and the environment.

### Example Tools & References

* MITRE ATT&CK Framework
* MITRE EMB3D
* Consultant Attack Surface and Threat Modeling Tools/Methodology/Analysis
* Hacking Exposed ICS OT IoT Consequence, Threat, and Attack tables
* MITRE TARA
* Bowtie
* Nmap
* Nessus
* Kali
* Networkminer
* Wireshark
* BinaryNinja, ObjectSecurity, Ghidra
* PowerShell, Windows SystemInternals, and Linux command line tools
* Grassmarlin
* OWASP ZAP
* Remnux, Cuckoo & Volatility
* Vendor documentation, tools
* CVSS calculator
* ICS OT IoT-CERT and US-CERT alerts
* MITRE CVE and NIST NVD
* MITRE CWE
* NIST SP 800-82, 53, 160 and 161
* DHS CSET
* DoD Mission Assurance Vulnerability Assessment Benchmarks 2014
* USCYBERCOM ACI TTPs
* AEM PARRE tool
* Exida CyberPHAx tool
* Customer documentation
* RedTiger’s Redcat tool for Windows host information gathering
* Nipper-NG

### Required deliverables from Customer

* Access to network span/mirror ports for passive sniffing and packet captures
* Access to network active ports and applicable workstations, HMIs, servers, firewalls, gateways for scanning
* Access to all requested documentation, systems, logs, site locations, and personnel to support running of tools and providing equivalent level of information
* Temporary admin accounts on applicable assets for assessment or support from personnel with admin access to required assets to run necessary tools that may require a temporary admin account to run
* Access to third parties and vendor software, documentation, tools such as ICS OT IoT vendor manuals, technical specifications, diagrams, spare parts equipment for offline analysis etcetera (includes access to viewing logic of PLCs, RTUs, HMIs etc.)
* Known IP address ranges, device names and MAC addresses, diagrams (system, network, instrumentation), list of ICS OT IoT vendor product types, brands, and known ICS OT IoT protocols etcetera

### Consultant Deliverables

* Customer specific CVSS scoring of discovered vulnerabilities that impact specific ICS OT IoT assets and operations at specific in scope sites and impact to specific business mission objectives, business units etcetera
* Recommendations to reduce consequences, impacts, and risks as well as counter vulnerabilities and threats to ICS OT IoT assets and operations
* Understanding of installed software, connections to and from ICS OT IoT assets, accuracy of diagrams, ports, protocols, and services etcetera

## Physical Tour Boots on the Ground Assessments

This is used to gain eyes on the ICS OT IoT assets and critical operations on the ground at critical sites. It is necessary in ICS OT IoT and the primary difference between an ICS OT IoT security risk assessment and a traditional IT corporate risk assessment. Going into the field operations separates assumptions and outdated documentation from reality.

### Example Tools & References

* DHS CSET
* DoD Mission Assurance Vulnerability Assessment Benchmarks 2014
* USCYBERCOM ACI TTPs
* Digital Camera
* Notebooks
* Personal Protective Equipment (PPE) as needed
* ICS OT IoT vendor documentation
* ICS OT IoT asset diagrams and site information
* AEM PARRE tools
* Exida CyberPHAx tool
* Bowtie
* Physical Red Teaming Methodology, Analysis and Tools

### Required deliverables from Customer

* Access to critical site locations, personnel, documentation, and ICS OT IoT assets
* Correct points of contact at each site and for each ICS OT IoT system, asset, process etcetera

### Consultant Deliverables

* Pictures of ICS OT IoT assets and adjacent applicable assets including configurations, physical locations, conduits etcetera
* Mapping of pictures to site narratives, vulnerabilities, threats, consequences, impacts, and risks
* Understanding of accuracy of diagrams and information provided by customer and third parties

## Threat, Consequence, Impact, Vulnerability, Interdependency, Risk Analysis

This is used to analyze all gathered information about the organization and its ICS OT IoT operations and assets. This is where that information is used to map ICS OT IoT assets, people, processes and technologies to vulnerabilities, threats, consequences, and impacts.

### Example Tools & References

* Bowtie
* AEM PARRE tool
* Exida CyberPHAx tool
* HAZOP and PHA information
* ICS OT IoT vendor documentation
* Microsoft Threat modeling tools
* MITRE ATT&CK Framework
* MITRE TARA
* MITRE CVSS calculator
* IVSS tool
* DHS CSET
* DoD Mission Assurance Vulnerability Assessment Benchmarks 2014
* USCYBERCOM ACI TTPs
* Consultant Attack Mapping Threat Modeling Analysis, Tools, Methodology

### Required deliverables from Customer

* Access to requested personnel, documents, sites, third parties, technology, and assets

### Consultant Deliverables

* Initial Threat models of attack paths to ICS OT IoT assets and operations specific to discovered vulnerabilities
* Mapping of consequences, impacts, threats to vulnerabilities and risks to ICS OT IoT assets and operations
* Understanding of threats and vulnerabilities and their countermeasures

## Recommendations

This is used to break out discovered risks into actionable and mitigative risk, consequence and impact reduction tasks that can counter threats and vulnerabilities.

### Example Tools & References

* NIST Cybersecurity Framework
* NIST SP 800-82
* MITRE TARA
* MITRE ATT&CK Framework
* ISA/IEC 62443
* ISA84.00.09
* PLC Top 20 Secure Coding Practices
* OWASP
* STIGS and CIS Benchmarks
* POA&Ms and Mitigation Roadmaps
* ICS OT IoT Consequence, Impacts, Threats, Attacks tables from Hacking Exposed ICS OT IoT
* DHS CSET
* DoD Mission Assurance Vulnerability Assessment Benchmarks 2014
* USCYBERCOM ACI TTPs

### Required deliverables from Customer

* Access to requested people, information, documentation, sites, and assets

### Consultant Deliverables

* High level recommendations mapped to each site
* Detailed appendix of complete list of all total recommendations mapped to consequences, threats and vulnerabilities discovered

## Optional Red Team Penetration Testing (additional scope and cost)

* External Penetration Test (Black Box)
* Internal Penetration Test (Gray Box)
* Comprehensive Vulnerability Discovery/Assessment (White Box)

While Consultant approach conforms to many often-referenced industry standard mythologies such as: OWASP, PTEST, OSSTMM, ISECOM, NIST SP 800-115 and others, we also draw from a highly experienced community of ICS OT IoT focused penetration red teamers who have decades of experience penetration testing ICS OT IoT assets specifically to help Consultant deliver a highly targeted and specialized red team penetration test.

A high-level description of the methodology and project flow is as follows:

**External Testing**

An overall risk profile of the client will be created using open source intelligence (OSINT) tools and methods. The purpose is to discover how much publicly available information is exposed that could assist an attacker and potentially lead to a security breach.

OSINT tools Consultant and red team expert partners typically uses:

* Google
* Shodan
* Maltego
* Whois
* Spartan
* Kali Linux Discovery Tools
* Variety of publicly available websites
* Custom ICS OT IoT scripts (both open source and consultant made)

Active “black box” external testing is an attempt to discover and active attempts to exploit vulnerabilities in assets that are exposed to the internet (intentionally or otherwise). Once vulnerabilities are discovered, exploitation is not attempted unless approval is written into the rules of engagement. Once an asset is compromised, further lateral movement by pivoting from the compromised asset is not performed unless permission to do so is written into the rules of engagement or other written permission is granted.

Consultant and red team partners uses the following tools for scanning, enumerating, and exploiting vulnerabilities for external testing:

* Nmap
* Nessus
* Recon-NG
* Spiderfoot
* Spartan
* BurpSuite
* Metasploit
* Exploit Pack
* Custom ICS OT IoT scripts (both open source and consultant made)
* Kali Linux (multiple standard tools)

**Internal Testing**

At this point, we stage the test as if the attacker is on the internal network (especially ICS OT IoT). If exposures were found in external/adjacent networks, it is not recommended to continue to pivot directly onto the production ICS OT IoT systems without express permission and careful monitoring and coordination. For internal testing and assessment, all or a combination of the following methods are used:

* Active vulnerability scanning
* Document/configuration review
* Physical walk-around
* Penetration testing/active exploitation
* RF/wireless scanning/exploitation

Notes on internal methods:

* This stage typically assumes the attacker is in or there is an insider threat (including malicious media)
* We are focusing on validating (or finding) vulnerabilities and exploits that pose a valid and meaningful risk to the business, safety, and production (overriding or altering safety logic, disabling critical controls, etc.)

Consultant uses the following tools for scanning, enumerating, and exploiting vulnerabilities for internal testing:

* Nmap
* Nessus
* Recon-NG
* Spiderfoot
* Spartan
* BurpSuite
* Metasploit
* Exploit Pack
* Kali Linux (multiple standard tools)
* Security Onion (ELK, Snort, Bro, Suricata)
* HackerRF (Radio Communication), RTL-SDR, Ubertooth One, Flipper Zero etc.
* LAN Turtle and Packet Squirrel (Physical Red Team Engagements Only)
* Tenable OT
* Custom ICS OT IoT scripts (both open source and consultant made)

**ICS OT IoT Specific Testing**

The following strategies and attack vectors are considered when penetration testing ICS OT IoT equipment and networks (contingent upon approval and being in scope):

* Test device robustness using packet crafting and fuzzing using
  + Crafted malformed packets using Netcat, hping3, Nping, and Scapy
  + Vulnerability Scanners such as Nessus and Nexpose, which contain pre-canned DoS scans that can be used to test on devices
  + Fuzzers (such as Peach Fuzzer), which can test a multitude of data mutations, automatically reset the device when needed, and record the results
* MITM attacks to sniff traffic and attempt “record and replay” and altering data “on the fly” control
* Vendor remote communication and engineering applications to find logic flaws, bypass authentication, and analyze functionality
* Known and zero-day vulnerabilities
  + Attempt to exploit known CVE/ICS OT IoT-CERT advisory vulnerabilities
  + Attempt to compromise devices and modules running outdated, vulnerable operating systems
  + Perform reverse engineering, fuzzing, and vulnerability research on vendor applications used for device communication
  + Reverse engineer firmware in search of hard coded credentials and private keys (which is not that uncommon) and backdoors as well as zero-day vulnerabilities (coding bugs)
  + Attempt to create “trojanized” malicious firmware that can be downloaded and accepted by the device

While the same penetration testing skills and methodologies are used to test ICS OT IoT servers and workstations as they are with business IT systems, the following ICS OT IoT specific strategies are considered when testing these systems (contingent upon approval and being in scope):

* Attempt to compromise SCADA servers (e.g., application servers, tag databases) to intercept, control, and spoof data back to the HMI
* Use MITM attacks to attempt to hijack control of ICS OT IoT devices and spoof data back to the HMI
* Compromise the tag database to cause operators to inadvertently perform harmful actions (e.g., close a valve on an already over pressurized pipe instead of opening it)
* Compromise engineering workstations in search of credentials or to alter the logic on devices
* Attempt to exploit known CVE/ICS OT IoT-CERT advisory vulnerabilities (Just as we mentioned, know and study ICS OT IoT-CERT advisories)
* Reverse engineer vendor applications in search of zero-day vulnerabilities or to replicate their functionality for crafted intelligent attacks

**Social Engineering**

Social engineering takes advantage of one of the weakest links in any security program, the human factor. The SOW stated that carefully monitored social engineering is within the scope of this project. Therefore, the following social engineering methods will be considered:

* Use of “spear phishing,” social media vectors, and planting infected social media using specialized tools such as:
  + The Social Engineering Toolkit (SET)
  + The Browser Exploitation Framework (BeEF)
  + USB Rubber Ducky
  + Custom proprietary scripts and macros

**Sampling Like-Configured Systems**

It is infeasible to test and/or replicate the entire enterprise and production networks in a lab. The goal is to get a sampling of each unique setup and configuration for each type of device, server, and workstation. The goal is to represent each unique server and workstation setup in terms of hardware, operating system, applications, permissions, and other setup configurations.

**Risk Scenarios**

Vulnerability assessment and penetration testing projects often produce many findings. It can be difficult to determine which findings are false positives and, in cases where there is an extremely large amount of vulnerabilities, it can be a challenge to build a prioritized remediation plan for each one. Consultant and red team partners specialized in ICS OT IoT uses a strategy that groups findings into risk scenarios also known as “attack trees.” A risk scenario is comprised of one or more effected assets, vulnerabilities, data communication paths, and attack vectors that “tell the story” of how those assets could be exploited and how easy or difficult it might be. This scenario is then combined with given “criticality ratings” established for each asset, along with potential consequences and impacts, to provide a more efficient targeted prioritization of risks, rather than a listing of arbitrary values/ratings and/or CVSS scores.

# Deliverable Materials

Consultant will provide the client with a final report containing the following:

* **Executive summary/score card** with the top 10 most common findings across all in scope sites, listed in priority along with brief descriptions and risk rating score.
* **Detailed ICS OT IoT security risk report**, which contains the following:
  + Executive Narratives of the organization and each in scope site
  + Breakdown of discovered vulnerabilities in people, process, and technology
  + Pictures of applicable ICS OT IoT systems, devices, and assets as well as adjacent systems with impact to ICS OT IoT assets and operations
  + High level list of recommendations for the organization and each in scope site
  + Detailed Appendix of observed or discovered vulnerabilities, threats, risks, consequences, and impacts mapped to recommendations within each security control functional area (e.g., Access Control, Configuration Management etc.)
  + CVSS score using CVSS calculator for major
  + Lists of points of contacts for each business area, system, asset and in scope site
  + Appendices of recommended ICS OT IoT specific security trainings, certifications, roles, and responsibilities

# Consultant Responsibilities

* Consultant shall provide customer with ICS OT IoT security risk assessment consulting services and experts.
* Consultant shall at no time during this engagement configure, log into, implement, touch, or otherwise interact with any of Client’s infrastructure or equipment without express permission and careful coordination.
* The assessment is limited to in scope sites, ICS OT IoT assets and operations, adjacent systems and operations that impact ICS OT IoT and necessary third parties with impact to ICS OT IoT
* Implementation of recommendations to remediate discovered risks is not included in this engagement/SoW.
* Additional modification of tasks or scope will result in the opportunity being considered a separate engagement offering that will require additional scoping, additional costs and/or change order.
* Consultant will provide its own tools mentioned in this SoW
* Consultant will ensure advanced red team consultants have ICS OT IoT experience if optional red team is selected by customer.

# Customer Responsibilities

* Customer will designate one (1) employee to serve as a primary authoritative point of contact (POC) at the organizational level for the project. The POC will be responsible for enabling consultant to schedule customer resources for required meetings, interviews, and other needs deemed necessary to complete the project work as scoped. The POC will participate in status meetings as required and will serve as the first point of escalation for any project-related requests or issues.
* Customer will provide access to all proprietary information, applications, site locations, assets, systems and third parties necessary to complete the Scope of Work.
* Customer and customer resources will execute all data gathering activities in an efficient manner, and data will be promptly submitted to consultant consultants within a commercially reasonable response time. Any delays incurred in acquiring this information may result in the need for a Change Order and rescheduling of the project, at the discretion of consultant.
* Customer will provide the necessary staff availability to complete identified tasks and/or to participate in interviews. Customer’s inability to provide this staff may affect the completion of tasks and/or deliverables.
* Customer will provide access to any necessary facility and/or remote access to complete the project.

# Fee Schedule

This engagement will be conducted as a fixed cost plus contract. The total value for the Services pursuant to this SoW shall not exceed the cost listed below unless otherwise agreed to by both parties via the project change control procedure, as outlined within. A Project Change Request (PCR) will be issued specifying the amended value.

This figure is based on the timeline and scope of work outlined in this document. Consultant will provide the ICS OT IoT security consultant, tools and deliverables outlined in this SoW. The fixed cost does not include the optional advanced red team active exploitation penetration test.

| Item Description | Estimated Project Total |
| --- | --- |
| **ICS OT IoT security risk assessment services and deliverables** | **$** |

# Out-of-Pocket Expenses / Invoice Procedures

Consultant additional payment terms should be defined here. Include penalties for late payments etc.

# Assumptions

The following assumptions are observed throughout this engagement:

* Consultant assumes that the engagement will be partially conducted remotely as well as at location(s) specified within the scope of work. A Change Order may be required for any additional locations that require physical visitation by consultant but are not requested by Client during the project scoping process. In such cases Consultant may require the customer to cover the cost of the additional travel.
* Consultant assumes that the final deliverable report will be consistent with the items identified in the Deliverables section within this SoW. A Change Order fee will be applied to any additional reports that are required and are not included within this SoW.

# Project Change Control Procedure

The following process will be followed if a change to this scope of work (SOW) is required:

* A Project Change Request (PCR) will be the vehicle for communicating change. The PCR must describe the change, the rationale for the change, and the effect the change will have on the project SoW.
* The designated Project Manager of the requesting party (Consultant or Customer) will review the proposed change and determine whether to submit the request to the other party.
* Both Project Managers will review the proposed change and approve it for further investigation or reject it. Consultant and Customer will mutually agree upon any charges for such investigation, if any. If the investigation is authorized, the Customer Project Managers will sign the PCR, which will constitute approval for the investigation charges. Consultant will invoice Customer for any such charges, if any. The investigation will determine the effect that the implementation of the PCR will have on SOW price, schedule and other terms and conditions of the Agreement.
* Upon completion of the investigation, both parties will review the impact of the proposed change and, if mutually agreed, a Change Authorization will be executed.
* A written Change Authorization and/or PCR must be signed by both parties to authorize implementation of the investigated changes.