

AGENDA
SOUTHERN NEVADA AREA COMMUNICATIONS COUNCIL
BOARD OF DIRECTORS
REGULAR MEETING

10:00 AM – NOVEMBER 4, 2019
Las Vegas Valley Water District - Mead 3 Conference Room
1001 S. Valley View Blvd, Las Vegas, NV 89107
702-455-7390

ALL ITEMS LISTED ON THIS AGENDA ARE FOR ACTION BY THE BOARD OF DIRECTORS, UNLESS OTHERWISE INDICATED. ITEMS MAY BE TAKEN OUT OF ORDER. THE BOARD OF DIRECTORS MAY COMBINE TWO OR MORE AGENDA ITEMS FOR CONSIDERATION, AND/OR MAY REMOVE AN ITEM FROM THE AGENDA OR DELAY DISCUSSIONS RELATING TO AN ITEM ON THE AGENDA AT ANY TIME. COPIES OF WRITTEN MATERIALS PROVIDED TO THE BOARD MEMBERS IN ADVANCE OR AT THE MEETING MAY BE OBTAINED FROM DAVE GOSS, SNACC OFFICE, 6000 EAST ROCHELLE AVE, LAS VEGAS, NV OR BY CALLING (702) 455-7390.

COMMENTS BY THE GENERAL PUBLIC

NO ACTION MAY BE TAKEN: At this time, the Board of Directors will hear general comments from the public on matters under the jurisdiction of the Southern Nevada Area Communications Council.

ITEM NO.

1. FOR POSSIBLE ACTION: Approve the November agenda with the inclusion of tabled and/or reconsidered items, emergency items, and/or deletion of items, and approve the minutes of the September 23rd, 2019 meeting.
2. FOR DISCUSSION: Receive the Administrator's Report with the inclusion of the Strategic Plan Updates, SNACC Monthly Report for the month of August and September 2019, and a presentation by Jason Manzo on APCO and MTUG.
3. FOR POSSIBLE ACTION: Ratify the Administrator's execution of the Cooperative Management Agreement between United States Department of Interior, National Park Service and Southern Nevada Area Communications Council for radio console, hardware and software support, and other matters properly related thereto with the inclusion of Change 1, Change 2, and Change 3.
4. FOR POSSIBLE ACTION: Approve the Open Balances Procedures Policy.
5. FOR POSSIBLE ACTION: Amending the System Compatible Radios Policy to have Group Services in the list of features.
6. FOR POSSIBLE ACTION: Approve Purchase Order for the Bureau of Reclamation (BOR) to add an ASR (Astro Site Repeater) site at Hoover Dam.

Chair: Jeff Buchanan **Vice Chair:** Chris Vasquez

Board Members: Wendy Lotman, Scott Mazick, Bill Baltas, Frank Milligan,
Brian Nebeker, Brad Adams, Vincent Albowicz & Isaac Henn

AGENDA
SOUTHERN NEVADA AREA COMMUNICATIONS COUNCIL
BOARD OF DIRECTORS
REGULAR MEETING

7. FOR POSSIBLE ACTION: Approve the Motorola Change Order 9 to include Hoover Dam ASR (Astro Site Repeater) Site and Complimentary Basic Cyber Security Risk Assessment.

COMMENTS BY THE GENERAL PUBLIC

NO ACTION MAY BE TAKEN: At this time, the Board of Directors will hear general comments from the public on matters under the jurisdiction of the Southern Nevada Area Communications Council.

NEXT MEETING DATE/ADJOURN

LOCATIONS OF POSTING

This is a public meeting. In conformance with the Nevada Open Meeting Law, this agenda has been posted in the following locations:

Clark County Government Center – 500 S. Grand Central Parkway, Las Vegas, NV 89155

Clark County Water Reclamation District - 5857 E Flamingo Rd, Las Vegas, NV 89122

Clark County Courthouse - 200 Lewis Ave, Las Vegas, NV 89101

Las Vegas Valley Water District - 1001 S. Valley View Boulevard, Las Vegas, NV 89107

www.snacconline.com & <https://notice.nv.gov>

PLEASE POST

Chair: Jeff Buchanan **Vice Chair:** Chris Vasquez

Board Members: Wendy Lotman, Scott Mazick, Bill Baltas, Frank Milligan,
Brian Nebeker, Brad Adams, Vincent Albowicz & Isaac Henn

Southern Nevada Area Communications Council Agenda Item

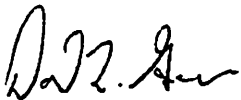
Issue: Approve the November agenda with the inclusion of tabled and/or reconsidered items, emergency items, and/or deletion of items, and approve the minutes of the September 23rd, 2019 meeting.	Date: November 4, 2019
Petitioner: David L. Goss, SNACC Administrator	Agenda Item: 1
Recommendation - FOR POSSIBLE ACTION: That the Board approve the November agenda with the inclusion of tabled and/or reconsidered items, emergency items, and/or deletion of items, and approve the minutes of the September 23rd, 2019 meeting and/or take action as necessary.	

Fiscal Impact: None

Background:

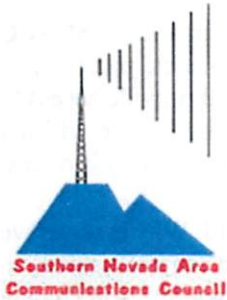
The Southern Nevada Area Communications Council operates an 800 megahertz (MHz) Public Safety radio communications system in the Clark County/Las Vegas urban area. This will be a reoccurring item.

Respectfully Submitted:



DAVID L. GOSS

SNACC Administrator



Southern Nevada Area Communications Council

MEETING MINUTES

Date: September 23, 2019

Location: Clark County Fire Department, Station 18
EOC Conference Room, 2nd Floor
575 E. Flamingo Rd
Las Vegas, NV 89119

Time: 1:31 P.M.

Board members present:

Jeff Buchanan, Chair	Chris Vasquez, Vice Chair
Frank Milligan	Scott Mazick
Isaac Henn	Wendy Lotman
Vincent Albowicz	

Call to Order

Public Comment: None

Introduction of the Board:

Unless otherwise stated, items may be taken out of the order presented on the agenda, and two or more items may be combined for consideration. The Board may also remove an item from the agenda or delay discussions relating to an item at any time

1. Approve the September agenda with the inclusion of tabled and/or reconsidered items, emergency items, and/or deletion of items, and approve the minutes of the August 28th, 2019 meeting. (**FOR POSSIBLE ACTION**):
 - A motion was made to approve; motion passed unanimously, one abstained.

2. Receive the Administrator's Report with the inclusion of the Strategic Plan Updates, SNACC Monthly Budget Report for the month of June and July 2019. (FOR POSSIBLE ACTION):

- David Goss – This contract is for the National Park Service to have access to our radio system and for SNACC to program their Security Radios. Also, to manage the radio dispatch center software updates, patches and diagnostics. We do not do the repair of their radios or any troubleshooting. Under B, we will provide access to partner agencies and system, they have about 30 radios, that we would program all radios, but we will not program more than those security radios. We removed *repair and troubleshoot and not program* their radios, those were the big changes.
- Jeff Buchanan – Why is it that we do not repair their radios, if you could clarify for the board. Why is it that we do not repair or program their radios? What were the catches that were made that the Board can understand, in other words, during this negotiation process there was originally a contract that was drawn up? After going through the contract with a fine-tooth comb and looking at a little bit more closely had to make sure that some things were tweaked and modified, can you explain that just so the board is aware so they can see what was included and what was excluded?
- David Goss – Again, that was part of what I mentioned earlier, we will not provide maintenance for their radios or their consoles, only software for their consoles. Also, it was in there that we were going to program all their radios, but we will program those 30 radios in their security but no more than that. The whole point of this process was to get an agreement with them and to get the money from previous SUA agreement, it totals \$215,000.
- Jeff Buchanan - I do have two more questions, Dave, if you could tell us this, do any of the other members of SNACC have this kind of sidebar agreement like they do with McIntosh, anybody else have that?
- Curtis Steadman, Motorola Solutions – There are some agencies that service through McIntosh but all of them go through Motorola for SUA.
- Chris Vasquez – For the consoles, Federal Government is the only one that uses McIntosh for maintenance of their equipment.
- Richard Johnson – Henderson Fire Department just entered a contract with McIntosh for maintenance of our radios.
- Jeff Buchanan - Thank you copy that, then the second question I have is, does this new agreement put the National Park Service in line with every other member of SNACC? In other words, they are paying for the same thing as year in, year out that the rest of the SNACC members.
- David Goss – It puts their dispatch center in line with their SUA like other SNACC members that have dispatch centers with their SUA.
- Scott Mazick – Dave, when we talk about the 5-year cost moving forward \$215,944.80, \$107,972.40 to catch up and \$107,972.40 for the next 5 years, is there a mechanism in place for this contract? What happens if there is an increase in SUA II fees in that 5 year, is there a mechanism in place to recoup those increases as well?
- Dave Goss – They would be issued an invoice just like anyone adding a console to their dispatch center, which would increase their SUA, it would not increase if they don't add equipment. Our SUA remains the same throughout our contract with Motorola unless they continue to add equipment.
- Scott Mazick – You mentioned that we would program their security radios, I think we should specify that in the contract that we will handle the 30 radios and no more than that. I would like to see that detailed out as possible.
- David Goss – Okay, we will have to get with them and change the contract. We talked to them quite a while ago about this and discussed with them that we would program their security radios at their security center.
- Scott Mazick – I think that should be documented as part of the agreement.
- David Goss – I will have to get with them and get a new change order for that.
- Scott Mazick – Okay.
- Jeff Buchanan – So let's explore that for a minute, so Steve, if this Board under that recommendation and understandably would have to be re-written, would this Board be able to approve with the amendment noted that Scott is suggesting or would we have to reconvene again, where are we at with that? Or could this Board say he, we agree with that amendment, go forth Dave and fulfill that and can we approve that or would we have to have another special meeting? Can you walk us thru the technical aspects of that?

- Steven Sweikert – No, the Board would have to approve in subsequent change order or amendment, the documents that are in front of us today have already been approved by the National Park Service so it would be a new amendment.
- Jeff Buchanan – So we would have to have another special meeting?
- Steven Sweikert – It would not have to be another special meeting, it could be a regular meeting. The reason we are having a meeting today is because of the timeline for Motorola.
- Jeff Buchanan – Okay, so again let's explore that, I think that that's adding something to the plate here right? So that means it's not ratified today, in which case we would need to again look to Motorola. It looks like an essence in spirit they are being good partners, The National Park Service. I think that Scott, you're pointing out some good details. It makes sense that the details are in writing, right? This is for everybody, this is for the National Park Service, this is for us and I think what's most important is that we have this discussion.
- David Goss – I read this incorrectly, if you read the change, it is not in there to program their radios. Originally, we had it in there that we would program their radios, but reading this change, it is not in the change order to program their security radios, so we are actually okay.
- Jeff Buchanan – So there is no intent to program their radios.
- David Goss – It is not in this change order to program their radios.
- Richard Johnson – But we are going to program 30 of them anyway?
- Dave Goss – No, it is not in this change order to do it.
- Jeff Buchanan –
- Frank Milligan – I thought that is what this discussion was about, that's what drove Scott's comment because you said you would program the radios.
- Dave Goss – I miss stated from up above that we would do it. But it is not in there to do that.
- Jeff Buchanan - Dave if I'm hearing you right, you're saying there is no intent by the agreement to program any of their radios, there is no need to detail. From the Boards perspective this again that this could be a two-way street and I don't think that this board or anyone needs to be receptive about moving it to another meeting. Here's the deal from the National Park Service, they may be under the understanding that you will program the 30 radios, right? So, what we don't want to say is that we can and then all the sudden that you're doing it and that just doesn't jive either.
- David Goss – When we discussed with them about 6 years ago, we said we would program their security radios, when they wrote this contract out, they put all their radios.
- Jeff Buchanan - Here's what I think, I'm hearing and please, I would like the input of the Board, I'm hearing confusion, the National Park Service might be under the impression that the 30 is still on the table. I think for the protection for both us and the National Park Service let's just put it in there. Our limiting factor, unless I am missing something, and please someone voice their opinion is that we are worried about the timetable and charges and timing on getting this approved.
- David Goss – We have time to get this amended.
- Frank Milligan – I keep hearing amendment, this has not been approved.
- Chris Vasquez – The original contract has been signed, this is an amendment to the contract. This is Change Order 1 of the original contract. What was presented today was already approved by the National Park Service.
- Jeff Buchanan - We are going to recommend that Dave, you put the recommendations for the second change order and bring it to the October 16th meeting and get this approved.
- Steve Sweikert – this could either be trailed to the next meeting or left as it is and put on the next agenda.
- Scott Mazick – Are payment milestones or payment dates specified on the contract?
- Chris Vasquez – On the original contract that was signed, it states that the \$21,594.40 would be paid yearly for five years. I wish the contract would have been presented for us to review, is there a copy for us to review really quick?
- David Goss – I did not bring it with me because it is about 43 pages long, I did not bring it with me.
- Jeff Buchanan – I'll add to that, as we look to have this on the next Board meeting, let's have the contract included for us to compare. For the next meeting we will do the trail option, with that we will go with having the 30 radios detailed and having the original contract in there for us to compare. Tabled for the next SNACC meeting.

COMMENTS BY THE GENERAL PUBLIC:

Jeff Buchanan – A quick shout out, thank you, Motorola for being so flexible. We really appreciate your partnership.

NEXT MEETING DATE/ADJOURN:

Next SNACC meeting: The next regular SNACC Board meeting will be held on October 16, 2019 at the Las Vegas Valley Water District.

Meeting adjourned at: 1:50 P.M.

Respectfully submitted:

Jeff Buchanan, Chairman
Attachments

Southern Nevada Area Communications Council Agenda Item

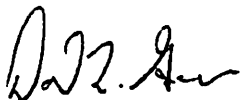
<p>Issue: Receive the Administrator's Report with the inclusion of the Strategic Plan Updates, SNACC Monthly Report for the month of August and September 2019, and a presentation by Jason Manzo on APCO and MTUG.</p>	<p>Date: November 4, 2019</p>
<p>Petitioner: David L. Goss, SNACC Administrator</p>	<p>Agenda Item: 2</p>
<p>Recommendation - FOR DISCUSSION: That the Board receive the Administrator's Report with the inclusion of the Strategic Plan Updates, SNACC Monthly Report for the month of August and September 2019, and a presentation by Jason Manzo on APCO and MTUG.</p>	

Fiscal Impact: None

Background:

The Board gave the request to the SNACC Administrator, on August 2015, to have the SNACC Budget presented in his Administrator's Report on a monthly basis. This was requested to inform the Board on the monthly SNACC expenses and to show what is currently available. This report includes any current system issues, deficiencies and/or updates. As of November 2017, a synopsis of the Strategic Plan reports are to be included as well.

Respectfully Submitted:



DAVID L. GOSS

SNACC Administrator

SNACC Administrators Report

November 4, 2019

SNACC BUSINESS:

SNACC continues to have weekly meetings with Nye County on the upgrade of the VHF Radios.

SNACC is also continuing with weekly meetings on the UNLV Project. This also includes discussions on UNLV on adding additional department users on the SNACC system.

Provided information on talkgroup usage for the FAO Dispatch Center, to be provided to the Fitch Communication Center Assessment.

SNACC has programmed 476 Radios for 24 different agencies since the last SNACC meeting.

Harris Radio has been working with SNACC to approve the use of their product on our system.

SNACC personnel also attended a Motorola Trunked Users Group (MTUG) meeting. This meeting demonstrates new equipment and also has discussions on radio issues.

Dave Goss attended training on Conducting Investigations. This was required training by Clark County.

SNACC is continuing to work with Las Vegas Metropolitan Police Department on day to day radio update information of alias changes and approving new ID's for encryption for SNACC users as well LVMPD users.

TECHNICAL ITEMS:

We are continuing investigations into a microwave upgrade project. This is necessary due to the age of the equipment and the advancement in technology. (Analog operations to Ethernet operations).

Over Labor Day weekend the Lake Mead site went down. This ended up being an issue with LVVWD T1 connection to the site, LVVWD technicians corrected the problem.

SNACC and LVMPD have had some interference issues recently, causing channels to be interfered with. We have been working together along with Motorola to find the cause of the interference.

OPEN RECEIVABLES:

Name	Invoice	Amount	Inv. Date	Description	Due Date	Days past due
CLV Fire & Rescue	90244912	\$11,258.57	5/29/2019	Console Maint: Yr5	6/29/2019	124
CLV Detention Ctr	90244915	\$12,544.57	5/29/2019	Console Maint: Yr5	6/29/2019	117
CLV Detention Ctr	90247059	\$44,595.72	7/10/2019	SNACC Radios	8/10/2019	82
Moapa Tribal PD	90247067	\$7,388.64	7/10/2019	SNACC Radios	8/10/2019	82

SNACC Administrators Report

BUDGET VARIANCES FOR THE MONTH OF AUGUST 2019:

BUDGET LINE ITEMS	Budget Amount	ACTUALS YTD	AUGUST ACTUALS	Last month's Remaining %	% Current	Justification
Cleaning/ Custodial	\$2,720.00	\$210.00	\$210.00	100%	92.3%	Mr. Janitorial
Equipment Maintenance and repair	\$12,500.00	\$1,520.00	\$1,520.00	100%	87.8%	DP AIR
Site Rentals	\$10,000.00	\$6,000.00	\$6,000.00	100%	41.6%	Payment to Las Vegas Valley Water District
Electricity for repeater sites	\$16,000.00	\$1,321.52	\$1,321.52	100%	91.70%	NV Power and Boulder City
Vehicle Maintenance	\$200,000.00	\$1,858.51	\$1,858.51	100%	90.70%	Jul-19
Tele- communications	\$9,880.00	\$1,067.33	\$1,042.33	100%	89.20%	United Teleservices, Telecom Fee, At&t, and Airwatch licenses.
Print/ Production	\$1,600.00	\$170.23	\$170.23	100%	89.40%	Konica Minolta Copier Charges

BUDGET VARIANCES FOR THE MONTH OF SEPTEMBER 2019:

BUDGET LINE ITEMS	Budget Amount	ACTUALS TO DATE	SEPTEMBER ACTUALS	Last month's Remaining %	% Current	Justification
Overtime	\$7,500.00	\$1,363.43	\$544.85	89.1%	81.8%	Jason and Jose were out programming and Daniela worked overtime.
Site Rentals	\$10,266.00	\$9,766.88	\$9,766.88	41.6%	4.9%	APEX site rental
Electricity for repeaters sites	\$16,000.00	\$2,681.33	\$1,359.81	91.70%	83.20%	NV Power and Boulder City
Print/Production	\$1,600.00	\$334.58	\$164.35	89.4%	79.1%	Konica Minolta Copier Charges

SNACC Administrators Report

SYSTEM REPORTS FOR THE MONTH OF AUGUST 2019:

Airtime – 2,943.4 (Hours)

Push to Talks – 2,272,135

Busies – 217 (6.90 min)

SYSTEM REPORTS FOR THE MONTH OF SEPTEMBER 2019:

Airtime – 2,943.4 (Hours)

Push to Talks – 2,197,532

Busies – 294 (9.90 min)

Southern Nevada Area Communications Council Agenda Item

<p>Issue: Ratify the Administrator's execution of the Cooperative Management Agreement between United States Department of Interior, National Park Service and Southern Nevada Area Communications Council for radio console, hardware and software support, and other matters properly related thereto with the inclusion of Change 1, Change 2, and Change 3.</p>	<p>Date: November 4, 2019</p>
<p>Petitioner: David L. Goss, SNACC Administrator</p>	<p>Agenda Item: 3</p>
<p>Recommendation - FOR POSSIBLE ACTION: That the Board ratify the Administrator's execution of the Cooperative Management Agreement between United States Department of Interior, National Park Service and Southern Nevada Area Communications Council for radio console, hardware and software support, and other matters properly related thereto with the inclusion of Change 1, Change 2, and Change 3 and/or take action as necessary.</p>	

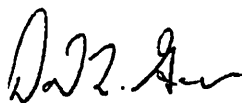
Fiscal Impact:

\$107,972.60 – As the SUA II yearly payments of \$21,594.52 are made to Motorola by SNACC, SNACC will then bill NPS for a reimbursement of payment. Under change 2 the billing cycles listed. Under change 3 the payments are due within 30 days of issuance.

Background:

On August 28, 2019 the Board made a motion to bring this item back to the Board for final approval of keeping the National Park Service on the SNACC system, if payment is received. The SNACC Administrator had been in communications with the National Park Service on having both agencies take the contract to their legal departments for review and approval. The National Park Service has agreed to pay SNACC \$107,972.40 one-time charges for computer and radio hardware that support NPS operations, per Article VI Interior National Park Service and Clark County, Southern Nevada Area Communications Council. On September 11, 2019 the National Park Service paid SNACC \$107,972.40. On September 23, 2019 the SNACC Board had an emergency meeting to ratify the Cooperative Management Agreement which includes the next five years of SUA II billing cycles. There were some changes that needed to be added to the Change 1 document. The Board tabled the agenda item for the next SNACC Board meeting on October 16, 2019. Change 2 was also received, however did not include specific radio count for security radios to be programmed, SNACC Administrator reached out to NPS for additional Change 3 to include radio count for programming 35 security radios and SUA payments due within 30 days of invoice issuance.

Respectfully Submitted:



DAVID L. GOSS
 SNACC Administrator

COOPERATIVE MANAGEMENT AGREEMENT G14081190001
BETWEEN
UNITED STATES DEPARTMENT OF INTERIOR
NATIONAL PARK SERVICE
AND
CLARK COUNTY, SOUTHERN NEVADA
AREA COMMUNICATIONS COUNCIL
DUNS NO.: 083782953
500 S GRAND CENTRAL PKWY, 6TH FLOOR
LAS VEGAS, NEVADA 89155

Project Title: Shared Use Radio Communications in Support of Public Safety
Amount of Federal Funds Obligated: \$215,944.80 (5 years + equipment)
Period of Performance: 09/01/2019 – 08/31/2024

THIS COOPERATIVE MANAGEMENT AGREEMENT is made and entered into by and between the Southern Nevada Area Communications Council (SNACC), and the UNITED STATES OF AMERICA, acting through the National Park Service (NPS). Throughout this agreement, both the NPS and the SNACC may be jointly referred to as the "Parties."

ARTICLE I – BACKGROUND AND OBJECTIVES

The objective of this Cooperative Management Agreement is to allow the NPS to be part of the SNACC, specifically allowing the shared use of radio communication, equipment, and services in support of the public safety.

ARTICLE II – AUTHORITY

A. NPS enters into this Cooperative Agreement pursuant to the following authorities:

1. **54 U.S.C. §101703 (a and b)** – The Secretary of the Interior is authorized to enter into an agreement with a State to provide for the cooperative management of the Federal and State park areas where a System unit is located adjacent to or near a State park area, and cooperative management between the NPS and a State will allow for more effective and efficient management of the System unit and State, provided that the Secretary does not transfer administration responsibilities for any System unit. Under a cooperative management agreement, the Secretary may acquire from and provide to a State agency goods and services to be used by the Secretary and the State in the cooperative management of land.
2. **54 U.S. Code § 101702 (d)** The Secretary may enter into cooperative agreements with State, local, or Tribal governments, other Federal agencies, other public entities, educational institutions, private nonprofit organizations, or participating private landowners for the purpose of protecting natural resources of System units through collaborative efforts on land inside and outside the System units.
3. **54 U.S.C. §§ 102701-102712** the NPS is authorized to render emergency rescue, fire-fighting, and cooperative assistance to nearby law enforcement and fire prevention agencies and for related purposes outside of the National Park System. Additionally, the Secretary of the Interior is authorized to designate officers and employees of any other

federal agency or law enforcement personnel of any state or political subdivision thereof, when deemed economical and in the public interest, and with the concurrence of that agency or that state or subdivision, to act as special police officers in areas of the National Park System when supplemental law enforcement personnel may be needed, and to exercise the powers and authorities delegated to NPS Rangers and US Park Police Officers.

B. SNACC enters into this agreement pursuant to:

- 1. Nevada Revised Statutes Chapter 277 or Joint Powers Agreement (JPA). NRS 277.180 – Interlocal Contracts.**

ARTICLE III – STATEMENT OF WORK

A. Background:

Lake Mead Interagency Communications Center (LMICC) manages emergency communications, public safety dispatching and is secondary public safety answering point for all federal land management agencies in Southern NV. This includes; four(4) NPS sites (Lake Mead NRA, Grand Canyon Parashant NM, Tule Springs Fossil Beds NM, and Great Basin NP), BLM law enforcement across the entire state of Nevada, USFS (Humboldt-Toiyabe NF), Bureau of Reclamation (Hoover Dam and other BOR lands within the Lower Colorado Region) and USFWS Desert Refuge Complex. This vast amount of land also hosts a large amount of visitation, use, crime and emergencies. It is located within and surrounding the Las Vegas Valley. These factors make for a wide variety of local, state and federal partners to provide law enforcement and emergency response. Each agency has a variety of frequencies across a varied spectrum. The need to communicate with each or multiple simultaneously is paramount for an appropriate and effective provision of public safety services. The local and county agencies coordinate through the Southern NV Area Communication Council. This entity manages radio frequencies for each agency as well as shared frequencies designated for multi-agency responses. The radio system is a proprietary network of towers, repeaters and associated computer components that must function together and must integrate into the radio consoles at the LMICC. Due system security needs, SNACC maintains the system and manages the system components. There is no other vendor that is able to provide the interoperability. The LMICC cannot procure the system components and build a link to interface due to encryption programming.

B. SNACC will provide the following:

- Direct access to the 800 MHz Public Service Radio System and indirect access to the 700 MHz Law Enforcement Radio System. Access provides interoperability with Local, State, and Federal Public Service and Law Enforcement Agencies**
- Program National Park Service dual-band radios with partner agency and interoperable frequencies managed by SNACC, as defined in radio frequency agreements**
- Manage Software User Agreement (SUA) and a hardware maintenance agreement for the LMICC dispatch console components**
- Provide Radio console (Motorola MCC7500) radio console software and hardware support, which includes, software and hardware updates, patches, diagnostics, troubleshooting and repair of radio issues**

- **SNACC Technicians will submit the personally identifiable information required by National Park Service to complete a thorough background check (signed releases and fingerprint cards)**

ARTICLE IV – TERM OF AGREEMENT

This Agreement shall become effective on 08/28/2019 through 08/27/2024, unless prior thereto it is terminated pursuant to the provisions of Article VIII hereof or of any applicable Federal or State law or regulation.

ARTICLE V – KEY OFFICIALS

A. Key officials are essential to ensure maximum coordination and communications between the parties for the work. They are:

1. For the NPS:

**a. Adam Kelsey
Lake Mead National Recreation Area
601 Nevada Hwy
Boulder City, NV 89005-2426
Adam_kelsey@nps.gov
(702) 293-8984**

**b. Brandon Marsmaker
Lake Mead National Recreation Area
601 Nevada Hwy
Boulder City, NV 89005-2426
Brandon_marsmaker@nps.gov
(702) 293-8937**

**c. Lila Klien
Lake Mead National Recreation Area
601 Nevada Hwy
Boulder City, NV 89005-2426
Lila_klien@nps.gov
(702) 293-8752**

2. For SNACC:

**a. David Goss
Clack County Info. Tech Dept.
500 South Grand Central Pkwy
Box 551700
(702) 455-7390**

B. Communications. The Parties shall address any communication regarding this Agreement to the key officials.

- C. Changes in Key Officials.** The Parties may make not any permanent change in a key official without written notice to the other party.

ARTICLE VI – EXPENDITURE OF FUNDS

- A. Funding:** The NPS will provide funding to the Clark County Information Tech Dept.; Attn: Accounts Receivable, 500 South Grand Central Pkwy. Box 651700, Las Vegas, NV 89155-1700 in an amount not to exceed \$21,594.48 per year for the work described in Article III and in accordance with the approved budget. In addition to the \$21,594.48, NPS agrees to pay a one-time payment of \$107,972.40 for computer and radio hardware that support NPS operations. Any award beyond the current fiscal year is subject to availability of funds.
- B. SNACC shall request payment in accordance with the following:**

- 1. Method of Payment:** Reimbursement through electronic fund transfer.
- 2. Requesting Reimbursement:** Requests for reimbursements must be submitted via mail or email – see addresses below. Invoices should not be submitted more than once monthly. Requests for reimbursement should coincide with normal billing patterns. Each request must be limited to the amount of disbursements made for the Federal share of direct project costs and the proportionate share of allowable indirect costs incurred during that billing period.

Mall or Email Invoices to:
Lake Mead National Recreation Area
Attn: Budget Office
601 Nevada Way
Boulder City, NV 89005
wendy_foster@nps.gov

- 3. Adjusting payment requests for available cash:** Funds that are available from repayments to, and interest earned on, a revolving fund, program income, rebates, refunds, contract settlements, audit recoveries, credits, discounts, and interest earned on any of those funds must be disbursed before requesting additional cash payments.
- 4. Bank Accounts:** All payments are made through electronic funds transfer to the bank account identified in the U.S Treasury system.

ARTICLE VII – PROPERTY UTILIZATION AND DISPOSITION

Any tools, equipment, material or other property supplied by an agency shall remain its own. Each agency agrees to properly maintain and safeguard each other's property. Reimbursement or replacement for loss or damage to the other agency's property shall be handled in accordance with the responsible employee's agency policy.

ARTICLE VIII – MODIFICATION AND TERMINATION

- A.** This Agreement represents the entire understanding of the Parties. No prior oral or written understanding shall be of any force or effect with respect to those matters specifically covered in this Agreement. This Agreement may be modified only in writing executed by the Parties.

- B. Either party may terminate its participation in this Agreement by providing sixty days written notice to the other party

ARTICLE IX - GENERAL AND SPECIAL PROVISIONS

A. Non-Discrimination

All activities pursuant to this Agreement shall be in compliance with the requirements of Executive Order 11246, Title VI of the *Civil Rights Act of 1964*, as amended, (78 Stat. 252; 42 U.S.C. §§ 2000d *et seq.*); Title V, Section 504 of the *Rehabilitation Act of 1973*, as amended, (87 Stat. 394; 29 U.S.C. §794); the *Age Discrimination Act of 1975* (89 Stat. 728; 42 U.S.C. §§ 6101 *et seq.*); and with all other federal laws and regulations prohibiting discrimination on grounds of race, color, sexual orientation, national origin, disabilities, religion, age, or sex.

B. Lobbying Prohibition

18 U.S.C. § 1913, Lobbying with Appropriated Moneys - No part of the money appropriated by any enactment of Congress shall, in the absence of express authorization by Congress, be used directly or indirectly to pay for any personal service, advertisement, telegram, telephone, letter, printed or written matter, or other device, intended or designed to influence in any manner a Member of Congress, to favor or oppose, by vote or otherwise, any legislation or appropriation by Congress, whether before or after the introduction of any bill or resolution proposing such legislation or appropriation; but this shall not prevent officers or employees of the United States or of its departments or agencies from communicating to Members of Congress on the request of any Member or to Congress, through the proper official channels, requests for legislation or appropriations which they deem necessary for the efficient conduct of the public business.

C. Anti-Deficiency Act

31 U.S.C. § 1341 - Nothing contained in this Agreement shall be construed as binding the NPS to expend in any one fiscal year any sum in excess of appropriations made by Congress for the purposes of this Agreement for that fiscal year, or other obligation for the further expenditure of money in excess of such appropriations.

- D. Prohibition on Text Messaging and Using Electronic Equipment Supplied by the NPS While Driving Executive Order 13513, *Federal Leadership on Reducing Text Messaging While Driving* was signed by President Barack Obama on October 1, 2009 (ref. <http://edocket.access.gpo.gov/2009/pdf/E9-24203.pdf>). This Executive Order introduces a Federal Government-wide prohibition on the use of text messaging while driving on official business or while using Government-supplied equipment. Additional guidance enforcing the ban will be issued at a later date. In the meantime, please adopt and enforce policies that immediately ban text messaging while driving company owned or rented vehicles, government-owned or leased vehicles, or while driving privately owned vehicles when on government business or when performing any work for or on behalf of the federal government.

E. Employees, Consultant, Agents, Contractors and Subcontractors

1. Either party may engage consultants or contract administration personnel as subcontractors to perform, administer, or coordinate any task governed by this Agreement and the attachments hereto. Nothing in this Agreement shall be construed as preventing either party from utilizing as many employees as deemed necessary for the proper and efficient execution of this Agreement.
2. All third-party contracts and or subcontracts executed in furtherance of this Agreement shall follow any and all Federal or State laws regarding contracting.

F. Liability

1. The United States shall be liable, to the extent allowed by law, including the Federal Tort Claims Act, for claims for personal injuries or property damage resulting from the negligent or wrongful act or omission of any employee of the United States while acting within the scope of his or her employment, arising out of this Agreement.
2. The Southern Nevada Area Communications Council shall be liable, to the extent allowed by law, including the Federal Tort Claims Act, for claims for personal injuries or property damage resulting from the negligent or wrongful act or omission of any employee of the Southern Nevada Area Communications Council while acting within the scope of his or her employment, arising out of this Agreement.

G. Severability

If any one or more of the terms, provisions, promises, covenants or conditions of this Agreement shall to any extent be adjudged invalid, unenforceable, void or voidable, for any reason whatsoever by a court of competent jurisdiction, each and all of the remaining terms, provisions, covenants, promises, and conditions of this Agreement shall not be affected thereby and shall be valid and enforceable to the fullest extent permitted by law.

H. Disputes

1. This Agreement shall be construed and interpreted, as to both validity and performance of the Parties, in accordance with the laws of the United States.
2. In the event of any dispute arising under this Agreement, the injured party shall notify the injuring party in writing of its contentions by submitting a claim therefore.

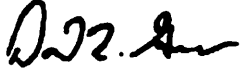
ARTICLE X – ATTACHMENTS

If there are attachments, they are incorporated into this Agreement. In the event of any apparent conflict between the terms of the Agreement and the attachments, the terms of the Agreement, including its designations and modifications, will prevail.

ARTICLE XI – AUTHORIZED SIGNATURES

IN WITNESS WHERE OF, the Parties hereto have signed their names and executed this Cooperative Management Agreement.

FOR SOUTHERN NEVADA AREA COMMUNICATIONS COUNCIL



Date 9-3-2019

David Goss
500 S. Grand Central Pkwy, 6th floor
Las Vegas, NV 89155-1700

FOR THE NATIONAL PARK SERVICE



Date 9/3/2019

Margaret Goodro, Superintendent
Lake Mead National Recreation Area
National Park Service

CHANGE 1
COOPERATIVE MANAGEMENT AGREEMENT G14081190001
BETWEEN
UNITED STATES DEPARTMENT OF INTERIOR
NATIONAL PARK SERVICE
AND
CLARK COUNTY, SOUTHERN NEVADA
AREA COMMUNICATIONS COUNCIL
DUNS NO.: 083782953
500 S GRAND CENTRAL PKWY, 6TH FLOOR
LAS VEGAS, NEVADA 89155

Project Title: Shared Use Radio Communications in Support of Public Safety
Amount of Federal Funds Obligated: \$215,944.80 (5 years + equipment)
Period of Performance: 09/01/2019 – 08/31/2024

Existing:

ARTICLE III – STATEMENT OF WORK

B. SNACC will provide the following:

- Direct access to the 800 MHz Public Service Radio System and indirect access to the 700 MHz Law Enforcement Radio System. Access provides interoperability with Local, State, and Federal Public Service and Law Enforcement Agencies
- Program National Park Service dual-band radios with partner agency and interoperable frequencies managed by SNACC, as defined in radio frequency agreements
- Manage Software User Agreement (SUA) and a hardware maintenance agreement for the LMICC dispatch console components
- Provide Radio console (Motorola MCC7500) radio console software and hardware support, which includes, software and hardware updates, patches, diagnostics, troubleshooting and repair of radio issues
- SNACC Technicians will submit the personally identifiable information required by National Park Service to complete a thorough background check (signed releases and fingerprint cards)

Change:

B. SNACC will provide the following:

- Direct access to the 800 MHz Public Service Radio System and indirect access to the 700 MHz Law Enforcement Radio System. Access provides interoperability with Local, State, and Federal Public Service and Law Enforcement Agencies
- Allow National Park Service access to partner agency and interoperable frequencies managed by SNACC, as defined in radio frequency agreements
- Manage Software User Agreement (SUA)
- Provide radio console (Motorola MCC7500) software and hardware support, which includes, software and hardware updates and patches

- SNACC Technicians will submit the personally identifiable information required by National Park Service to complete a thorough background check (signed releases and fingerprint cards)

ARTICLE XI – AUTHORIZED SIGNATURES

IN WITNESS WHERE OF, the Parties hereto have signed their names and executed this Cooperative Management Agreement.

FOR SOUTHERN NEVADA AREA COMMUNICATIONS COUNCIL

David Goss
500 S. Grand Central Pkwy, 6th floor
Las Vegas, NV 89155-1700

Date _____

FOR THE NATIONAL PARK SERVICE

Margaret Goodro

for Margaret Goodro, Superintendent
Lake Mead National Recreation Area
National Park Service

Date 9/19/2019

CHANGE 2
COOPERATIVE MANAGEMENT AGREEMENT G14081190001
BETWEEN
UNITED STATES DEPARTMENT OF INTERIOR
NATIONAL PARK SERVICE
AND
CLARK COUNTY, SOUTHERN NEVADA
AREA COMMUNICATIONS COUNCIL
DUNS NO.: 083782953
500 S GRAND CENTRAL PKWY, 6TH FLOOR
LAS VEGAS, NEVADA 89155

Project Title: Shared Use Radio Communications in Support of Public Safety
Amount of Federal Funds Obligated: \$215,944.80 (5 years + equipment)
Period of Performance: 09/01/2019 – 08/31/2024

Existing:

ARTICLE III – STATEMENT OF WORK

B. SNACC will provide the following:

- Direct access to the 800 MHz Public Service Radio System and indirect access to the 700 MHz Law Enforcement Radio System. Access provides interoperability with Local, State, and Federal Public Service and Law Enforcement Agencies
- Allow National Park Service access to partner agency and interoperable frequencies managed by SNACC, as defined in radio frequency agreements
- Manage Software User Agreement (SUA)
- Provide radio console (Motorola MCC7500) software and hardware support, which includes, software and hardware updates and patches
- SNACC Technicians will submit the personally identifiable information required by National Park Service to complete a thorough background check (signed releases and fingerprint cards)

Change:

B. SNACC will provide the following:

- Direct access to the 800 MHz Public Service Radio System and indirect access to the 700 MHz Law Enforcement Radio System. Access provides interoperability with Local, State, and Federal Public Service and Law Enforcement Agencies
- Allow National Park Service access to partner agency and interoperable frequencies managed by SNACC, as defined in radio frequency agreements
- Manage Software User Agreement (SUA)
- Provide radio console (Motorola MCC7500) software and hardware support, which includes, software and hardware updates and patches

- SNACC Technicians will submit the personally identifiable information required by National Park Service to complete a thorough background check (signed releases and fingerprint cards)
- Security Radios at Hoover Dam will be programed with interop channels for communications with outside agencies.
- Annual SUA bill due September 30
- Any additional consoles will have an SUA cost of \$1799.50

ARTICLE XI – AUTHORIZED SIGNATURES

IN WITNESS WHERE OF, the Parties hereto have signed their names and executed this Cooperative Management Agreement.

FOR SOUTHERN NEVADA AREA COMMUNICATIONS COUNCIL

David Goss
500 S. Grand Central Pkwy, 6th floor
Las Vegas, NV 89155-1700

Date _____

FOR THE NATIONAL PARK SERVICE

for 

Margaret Goodro, Superintendent
Lake Mead National Recreation Area
National Park Service

Date 10/2/2019

Southern Nevada Area Communications Council Agenda Item

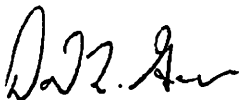
Issue: Approve the Open Balances Procedures Policy.	Date: November 4, 2019
Petitioner: David L. Goss, SNACC Administrator	Agenda Item: 4
Recommendation - FOR POSSIBLE ACTION: That the Board approve the Open Balances Procedures Policy and/or take action as necessary.	

Fiscal Impact: None

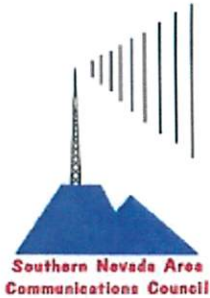
Background:

This policy was created due to SNACC having some issues collecting monies from an agency for five years. The SNACC Operations/Governance working group worked on this policy with the SNACC Administrator to avoid any type of issues with open balances in the future.

Respectfully Submitted:



DAVID L. GOSS
SNACC Administrator

<p style="text-align: center;">Southern Nevada Area Communications Council</p> <p style="text-align: center;">POLICIES AND PROCEDURES</p>	 <p style="text-align: center;">Southern Nevada Area Communications Council</p>
<p>Subject:</p> <p>Open Balances Procedures Policy</p>	<p>No. 2</p> <p>Effective Date</p>

1.0 Purpose

1.1. Defines the steps taken by the Southern Nevada Area Communications Council (SNACC) when participants have open balances beyond 90 days past due.

2.0 Owner

2.1. Southern Nevada Area Communications Council.

3.0 Applies To

3.1. SNACC members/participants that have an open balances due to SNACC.

4.0 Background

4.1. All invoices are sent out annually. The terms of payment are Net 30 days from the original invoice date.

4.2. Accounting sends out Past Due reminders every 30 (Thirty) days of the invoice date if the invoices remain unpaid.

5.0 Supporting Rules

5.1 All entities with open balances due to SNACC will continue to receive notices every 30 (Thirty) days from original invoices date.

5.2 A certified disconnection notice will be sent out to any entity if payment is not received within 120 days of the original invoice.

6.0 Responsibilities

6.1 The SNACC Administrator is responsible for advising the SNACC Board of Directors of recommendations related to open balances.

6.2 If the payment for the past due invoice is not received within the 120 days (240 from original invoice date) of the disconnection notice, the Southern Nevada Area Communications Council will take steps to disconnect the entity.

Southern Nevada Area Communications Council Agenda Item

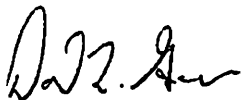
Issue: Amending the System Compatible Radios Policy to have Group Services in the list of features.	Date: November 4, 2019
Petitioner: David L. Goss, SNACC Administrator	Agenda Item: 5
Recommendation - FOR POSSIBLE ACTION: That the Board approve Amending the System Compatible Radios Policy to have Group Services in the list of features. and/or take action as necessary.	

Fiscal Impact: None

Background:

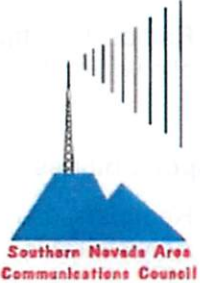
The System Compatible Radios Policy was created in October 2017 to guide our users towards purchasing radios with the necessary features to be ready for our upgraded system. Group Services allows over the air firmware and flashcode changes/updates. (Jason will provide a PowerPoint with more information).

Respectfully Submitted:



DAVID L. GOSS

SNACC Administrator

<p>SOUTHERN NEVADA AREA COMMUNICATIONS COUNCIL POLICIES AND PROCEDURES</p>	 <p>Southern Nevada Area Communications Council</p>
	<p>No. 1</p>
<p>Subject: SNACC System Compatible Radios</p>	<p>Effective Date 10/18/2017 Revised on: 10/16/2019</p>

1.0 Purpose

- 1.1. Defines a policy and process for the use of compatible branded radios to be used on the SNACC system.

2.0 Owner

- 2.1. SNACC Operations/Governance Working Group (OGWG).

3.0 Applies To

- 3.1. Entities requesting to use P25 compatible branded radios on the SNACC system.

4.0 Background

- 4.1. With the upgrade to P25 operations, the SNACC system is no longer a proprietary system and other brand radios may work with perhaps some limitations.

5.0 Policy Statement

- 5.1. The SNACC will test and approve non-Motorola radios to be used on the SNACC system. All non-Motorola radios must be approved by SNACC Board.

6.0 Supporting Rules

- 6.1. A SNACC user may request to use a non-Motorola radio on the system.
- 6.2. Any non-Motorola radio will be thoroughly tested by the Technical Working Group (TWG) and SNACC technicians, for proper operations on the system.
- 6.3. Any features that will not be available to the affected user will be brought to their attention.

6.4. Radios that have not gone through the SNACC performance evaluation will not be allowed on the system.

7.0 Responsibilities

7.1. Requests use non-Motorola radios on the system must be submitted to the SNACC Administrator.

7.2. Submissions must include:

7.2.1. Agency name and single point of contact.

7.2.2. Any special needs or applications (i.e., Emergency, Encryption, or other functions required).

7.2.3. All brands and models must have complete specifications to work on P25 system.

7.2.4. Customer is responsible for bringing in equipment ready for testing.

7.3. The Administrator will provide the SNACC Board with an evaluation of the unit's performance and request an approval/disapproval of acceptance.

7.3.1. The SNACC Administrator will inform the requesting user, in writing, of the evaluation results, and the SNACC Boards decision.

8.0 Conditions for Exemption or Waiver

8.1. As provided in the Waiver or Exception Policy.

9.0 Applicable Policies and/or Procedures

9.1. As listed at <http://snacconline.com/about-us/>

NON-LAW ENFORCEMENT

DESCRIPTION REQUIREMENTS

PORTABLE and MOBILE RADIOS
DIGITAL
P25 TRUNKING
ADVANCED SYSTEM KEY - HARDWARE KEY
TDMA OPERATION (Phase II)
PROGRAMMING OVER P25 (OTAP)
RADIO MANAGEMENT ONLINE
GROUP SERVICES

LAW ENFORCEMENT

METRO DESCRIPTION REQUIREMENTS

PORTABLE and MOBILE
DIGITAL
P25 TRUNKING
ADVANCED SYSTEM KEY - HARDWARE KEY
TDMA OPERATION (Phase II)
PROGRAMMING OVER P25 (OTAP)
OTAR W/MULTIKEY
AES ENCRYPTION
RADIO MANAGEMENT ONLINE
GROUP SERVICES

Issue: Approve Purchase Order for the Bureau of Reclamation (BOR) to add an ASR site at Hoover Dam.	Date: November 4, 2019
Petitioner: David L. Goss, SNACC Administrator	Agenda Item: 6
Recommendation - FOR POSSIBLE ACTION: That the Board approve Purchase Order for the Bureau of Reclamation (BOR) to add an ASR site at Hoover Dam. and/or take action as necessary.	

Fiscal Impact: \$559,335.00 – All of which will be refunded back to SNACC. If accepted, the contracts with Motorola for Maintenance and SUA II would increase (See table below) Year 1 is not shown because it would be covered under warranty. This would be from March 2020 to March 2021.

POST WARRANTY SUPPORT ESTIMATES

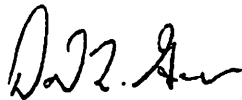
The below pricing is for information only and will be added to the existing support agreement per the terms of the agreement.

	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8
Maintenance	\$16,492.00	16,986.76	\$17,496.36	\$18,021.25	\$18,561.89	\$19,118.75	\$19,692.31
SUA II	\$8,399.51	\$8,404.51	\$8,410.51	\$8,415.51	\$8,421.51	\$8,426.51	\$8,432.51
Total	\$24,891.51	\$25,391.27	\$25,906.87	\$26,436.77	\$26,983.40	\$27,545.26	\$28,124.82

Background:

The SNACC Administrator has been working with James Roach, BOR Representative for the Hoover Dam on creating a contract/agreement for the site to be added to the Hoover Dam. These discussions have been going on for about 5 years.

Respectfully Submitted:



DAVID L. GOSS
 SNACC Administrator

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 3

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER 09/09/2019	2. CONTRACT NO. (If any)	6. SHIP TO:	
		a. NAME OF CONSIGNEE Mr. James (JR) Roach, 702-494-2482	
3. ORDER NO. 140R3019P0062	4. REQUISITION/REFERENCE NO. 0040443650		
5. ISSUING OFFICE (Address correspondence to) Bureau of Reclamation Lower Colorado Region Regional Office 500 Fir Street Boulder City NV 89005		b. STREET ADDRESS Bureau of Reclamation-LC-Hoover Dam Hoover Dam Central Warehouse State Route 172	
		c. CITY Boulder City	d. STATE NV
		e. ZIP CODE 89005-0400	

7. TO ATTN GOVERNMENT POC		f. SHIP VIA	
a. NAME OF CONTRACTOR CLARK, COUNTY OF		8. TYPE OF ORDER	
b. COMPANY NAME %Southern Nevada Area Communications Council		<input checked="" type="checkbox"/> a. PURCHASE	<input type="checkbox"/> b. DELIVERY
c. STREET ADDRESS 500 S GRAND CENTRAL PKWY 6 FL		REFERENCE YOUR: Quote dated 08/28/2019	
d. CITY LAS VEGAS		Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated	
e. STATE NV	f. ZIP CODE 89155-4502	Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract	

9. ACCOUNTING AND APPROPRIATION DATA 01		10. REQUISITIONING OFFICE BOR-LC-Hoover Dam	
11. BUSINESS CLASSIFICATION (Check appropriate box(es))			12. F.O.B. POINT
<input type="checkbox"/> a. SMALL <input checked="" type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED <input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM <input type="checkbox"/> h. EDWOSB			
13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date) 03/31/2020
a. INSPECTION Destination	b. ACCEPTANCE Destination	16. DISCOUNT TERMS	

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	NAICS: 515111 Project Title: Public Safety Radio Service Access for Hoover Dam Security Zone Legacy Doc #: BOR Continued ...					

18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		17(h) TOTAL (Cont. pages)
21. MAIL INVOICE TO:						
a. NAME Invoice Processing Platform System						\$559,335.00
b. STREET ADDRESS (or P.O. Box) US Department of Treasury http://www.ipp.gov						
c. CITY		d. STATE	e. ZIP CODE		\$559,335.00	17(i) GRAND TOTAL

22. UNITED STATES OF AMERICA BY (Signature) 	23. NAME (Typed) Kevin Broadnax TITLE: CONTRACTING/ORDERING OFFICER
---	---

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE NO

2

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

ORDER NO.

140R3019P0062

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
00010	<p>Admin Office: Bureau of Reclamation Lower Colorado Region Regional Office 500 Fir Street Boulder City NV 89005</p> <p>Account Assignm: K G/L Account: 6100.257J0 Business Area: R000 Commitment Item: 257J00 Cost Center: RR03132200 Functional Area: R19520000.000000 Fund: 19XR0680A5 Fund Center: RR03132200 Project/WBS: RX.19520002.3VK0742 PR Acct Assign: 01 Period of Performance: 09/09/2019 to 03/31/2020</p> <p>Public Safety Radio Service Access in Hoover Dam Security Zone</p> <p>All work shall be performed in accordance with the attached Performance Work Statement. This is a Firm-Fixed Price Task Order.</p> <p>All payment requests shall be submitted electronically, after delivery of items/submittals or completion of services, to the Invoice Processing Platform (IPP) at https://www.ipp.gov/. Please e-mail a copy of the contractor-generated invoice to the Contracting POC concurrently with your submission. If you have any questions regarding payment, please contact the Contracting POC listed below.</p> <p>Points of Contact- Vendor: Mr. David Goss, 702-455-7390 or DDG@clarkcountynv.gov Government Technical: Mr. James (JR) Roach, 702-494-2482 or jroach@usbr.gov Government Contracting: Ms. Jennalyn Schilke, 702-293-8030 or jschilke@usbr.gov</p> <p>The total amount of award: \$559,335.00. The obligation for this award is shown in box Continued ...</p>				559,335.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

\$559,335.00

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE NO

3

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

ORDER NO.

140R3019P0062

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
17 (i) .						

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

\$0.00

CLAUSES

52.252-2 CLAUSES INCORPORATED BY REFERENCE - (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): FAR Clauses – <https://www.acquisition.gov/far/>

52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES - (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the date of the clause.

(b) The use in this solicitation or contract of any Department of the Interior Acquisition Regulation (48 CFR Chapter 14) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the name of the regulation.

52.212-4 CONTRACT TERMS AND CONDITIONS –COMMERCIAL ITEMS - (OCT 2018)
(Clause Above Incorporated by Reference)

ADDENDUM TO 52.212-4

52.204-4 PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER - (MAY 2011)

52.204-13 SYSTEM FOR AWARD MANAGEMENT MAINTENANCE - (OCT 2018)

52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES - (JUL 2018)

52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS - (DEC 2013)

52.233-4 APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM (OCT 2004)

52.242-15 STOP-WORK ORDER - (AUG 1989)

(Clauses Above Incorporated by Reference)

ADDENDUM TO 52.212-4

DOI-AAAP-0028 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS-INVOICE PROCESSING PLATFORM (IPP) - APR 2013)

Payment requests must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP).

'Payment request' means any request for contract financing payment or invoicing payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in the applicable Prompt Payment clause included in the contract, or the clause 52.212-4 Contract Terms and Conditions-Commercial Items included in commercial item contracts. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP invoice:

NONE. *See Note. _____

***NOTE: The Contractor shall also submit an electronic copy of the IPP invoice to the Contract Specialist at jschilke@usbr.gov once the invoice has been submitted to IPP. Failure to email the invoice may cause significant delay or possible rejection of your payment request.**

The Contractor must use the IPP website to register access and use IPP for submitting requests for payment. The Contractor Government Business Point of Contact (as listed in SAM) will receive enrollment instructions via email from the Federal Reserve Bank of Boston (FRBB) within 3-5 business days of the contract award date. Contractor assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email ippgroup@bos.frb.org or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the Contracting Officer with its proposal or quotation.

ADDENDUM TO 52.212-4

DOI-AAAP-0050 CONTRACTOR PERFORMANCE ASSESSMENT REPORTING SYSTEM - (DEC 2015)

- a. FAR 42.1502 directs all Federal agencies to collect past performance information on contracts. The Department of the Interior (DOI) has implemented the Contractor Performance Assessment Reporting System (CPARS) to comply with this regulation. One or more past performance evaluations will be conducted in order to record your contract performance as required by FAR 42.15.
- b. The past performance evaluation process is a totally paperless process using CPARS. CPARS is a web-based system that allows for electronic processing of the performance evaluation report. Once the report is processed, it is available in the Past Performance Information Retrieval System (PPIRS) for Government use in evaluating past performance as part of a source selection action.
- c. We request that you furnish the Contracting Officer (CO) with the name, position title, phone number, and email address for each person designated to have access to your firm's past performance evaluation(s) for the contract no later than 30 days after award. Each person granted access will have the ability to provide comments in the Contractor portion of the report and state whether or not the Contractor agrees with the evaluation, before returning the report to the Assessing Official (AO). Information in the report must be protected as source selection sensitive information not releasable to the public.
- d. When your Contractor Representative(s) are registered in CPARS, they will receive an automatically generated email with detailed login instructions. Further details, systems requirements, and training information for CPARS is available at <https://www.cpars.gov/>.
- e. Within 60 days after the end of a performance period, the AO will complete an interim or final past performance evaluation, and the report will be accessible at <https://www.cpars.gov/>.
 1. Contractor Representatives may then provide comments in response to the evaluation, or return the evaluation without comment.
 2. Your comments should focus on objective facts in the AO's narrative and should provide your views on the causes and ramifications of the assessed performance.
 3. All information provided should be reviewed for accuracy prior to submission.
 4. If you elect not to provide comments, please acknowledge receipt of the evaluation by indicating No comment in the space provided, and then selecting "Accept the Ratings and Close the Evaluation".

5. Your response is due within 60 calendar days after receipt of the CPAR. On day 15, the evaluation will become available in PPIRS-RC marked as "Pending" with or without comments and whether or not it has been closed.

6. If you do not sign and submit the CPAR within 60 days, it will automatically be returned to the Government and will be annotated: -The report was delivered/received by the contractor on (date). The contractor neither signed nor offered comment in response to this assessment.

f. The following guidelines apply concerning your use of the past performance evaluation:

1. Protect the evaluation as source selection information. After review, transmit the evaluation by completing and submitting the form through CPARS. If for some reason you are unable to view and/or submit the form through CPARS, contact the CO for instructions.

2. Strictly control access to the evaluation within your organization. Ensure the evaluation is never released to persons or entities outside of your control.

3. Prohibit the use of or reference to evaluation data for advertising, promotional material, pre-award surveys, responsibility determinations, production readiness reviews, or other similar purposes.

g. If you wish to discuss a past performance evaluation, you should request a meeting in writing to the CO no later than seven days following your receipt of the evaluation. The meeting will be held in person or via telephone or other means during your 60-day review period.

h. A copy of the completed past performance evaluation will be available in CPARS for your viewing and for Government use supporting source selection actions after it has been finalized.

ADDENDUM TO 52.212-4

1452.201-70 AUTHORITIES AND DELEGATIONS - (SEP 2011)

(a) The Contracting Officer is the only individual authorized to enter into or terminate this contract, modify any term or condition of this contract, waive any requirement of this contract, or accept nonconforming work.

(b) The Contracting Officer will designate a Contracting Officer's Representative (COR) at time of award. The COR will be responsible for technical monitoring of the contractor's performance and deliveries. The COR will be appointed in writing, and a copy of the appointment will be furnished to the Contractor. Changes to this delegation will be made by written changes to the existing appointment or by issuance of a new appointment.

(c) The COR is not authorized to perform, formally or informally, any of the following actions:

(1) Promise, award, agree to award, or execute any contract, contract modification, or notice of intent that changes or may change this contract:

(2) Waive or agree to modification of the delivery schedule;

(3) Make any final decision on any contract matter subject to the Disputes Clause;

(4) Terminate, for any reason, the Contractor's right to proceed;

(5) Obligate in any way, the payment of money by the Government.

(d) The Contractor shall comply with the written or oral direction of the Contracting Officer or authorized representative(s) acting within the scope and authority of the appointment memorandum. The Contractor need not proceed with direction that it considers to have been issued without proper authority. The

Contractor shall notify the Contracting Officer in writing, with as much detail as possible, when the COR has taken an action or has issued direction (written or oral) that the Contractor considers to exceed the COR's appointment, within 3 days of the occurrence. Unless otherwise provided in this contract, the Contractor assumes all costs, risks, liabilities, and consequences of performing any work it is directed to perform that falls within any of the categories defined in paragraph (c) prior to receipt of the Contracting Officer's response issued under paragraph (e) of this clause.

(e) The Contracting Officer shall respond in writing within 30 days to any notice made under paragraph (d) of this clause. A failure of the parties to agree upon the nature of a direction, or upon the contract action to be taken with respect thereto, shall be subject to the provisions of the Disputes clause of this contract.

(f) The Contractor shall provide copies of all correspondence to the Contracting Officer and the COR.

(g) Any action(s) taken by the Contractor, in response to any direction given by any person acting on behalf of the Government or any Government official other than the Contracting Officer or the COR acting within his or her appointment, shall be at the Contractor's risk.

ADDENDUM TO 52.212-4

WBR 1452.201-80 CONTRACTING OFFICER'S REPRESENTATIVE'S AUTHORITIES AND LIMITATIONS -- BUREAU OF RECLAMATION (MAY 2018)

(a) Performance of the work under this contract shall be subject to the technical direction of the Reclamation Contracting Officer's Representative (COR). The term "technical direction" is defined to include, without limitation:

(1) Inspecting and accepting or rejecting work performed under the contract.

(2) Representing the Government in technical phases of the work. The COR is responsible for the technical administration of the contract and will provide instructions and interpretations to the Contractor on all technical matters relating to the contract. The COR will supervise or oversee all Government technical and administrative personnel assigned to assist the COR.

(3) Reviewing and, where required by the contract, approving submittals of technical data, shop drawings, samples, literature, plans, or other data required to be delivered by the Contractor to the Government.

(b) The Contractor will receive a copy of the written COR designation from the Contracting Officer. It will specify the extent of the COR's authority to act on behalf of the Contracting Officer.

(c) Technical direction must be within the scope of work stated in the contract. Only the Contracting Officer is authorized to determine if a change is within the scope of the contract; therefore, the COR does not have the authority to, and may not, issue any technical direction that –

- (1) Constitutes a direction of additional work outside the Contract requirements;
- (2) Constitutes a change as defined in the contract clause entitled "Changes;"
- (3) In any manner causes an increase or decrease in the total contract cost, or the time required for contract performance;
- (4) Changes any of the expressed terms, conditions or specifications of the contract; or
- (5) Interferes with the Contractor's right to perform the terms and conditions of the contract.

(d) All technical direction shall be issued in writing by the COR.

(c) The Contractor must proceed promptly with the performance of technical direction duly issued by the COR in the manner prescribed by this clause and within its authority under the provisions of this clause. If, in the opinion of the Contractor, any instruction or direction by the COR falls within one of the categories defined in (c)(1) through (c)(5) of this clause, the Contractor must not proceed and must notify the Contracting Officer in writing within five (5) working days after receipt of any such instruction or direction and must request the Contracting Officer to modify the contract accordingly. Upon receiving the notification from the Contractor, the Contracting Officer must –

(1) Advise the Contractor in writing after receipt of the Contractor's letter that the technical direction is within the scope of the contract effort and does not constitute a change under the Changes clause of the contract; or

(2) Advise the Contractor that the Government will issue a written change order.

(f) A failure of the Contractor and Contracting Officer either to agree that the technical direction is within the scope of the contract or to agree upon the contract action to be taken with respect to the technical direction will be subject to the provisions of the clause entitled "Disputes."

ADDENDUM TO 52.212-4

WBR 1452.223-82 PROTECTING FEDERAL EMPLOYEES AND THE PUBLIC FROM EXPOSURE TO TOBACCO SMOKE IN THE FEDERAL WORKPLACE -- BUREAU OF RECLAMATION - (DEC 2009)

(a) In performing work under this contract, the contractor shall comply with the requirements of Executive Order 13058, dated August 9, 1997, which prohibits the smoking of tobacco products in all interior space owned, rented, or leased by the executive branch of the Federal Government, and in any outdoor areas under executive branch control in front of air intake ducts.

(b) In addition, pursuant to Federal Management Regulation (FMR) Bulletin 2009-B1, effective December 22, 2008, smoking is prohibited in courtyards and within 25 feet of doorways and air intake ducts on outdoor space under the jurisdiction, custody or control of GSA.

ADDENDUM TO 52.212-4

WBR 1452.237-80 SECURITY REQUIREMENTS--BUREAU OF RECLAMATION (FEB 2017)

(a) General Security Requirements:

(1) This clause addresses security requirements, including general procedural requirements, information security requirements, contractor employee suitability requirements, identification card requirements, site security requirements, vessel exclusion barriers, and information technology security requirements. Within this clause, COR means Contracting Officer's Representative. If there is no COR appointed and identified to the Contractor, the term instead will mean the Program Manager or any other authorized individual responsible for technical oversight under the contract. "Work site" means the Government facility, office, construction site, and any other area within the Government office or facility that the Contractor must access to accomplish work under this contract.

(2) The work performed under this contract shall only be accomplished by individuals (in the employment of the Contractor or any subcontractors) whose conduct and behavior is consistent with the efficiency of the Federal Service and the requirements of this contract, and who are acceptable to the CO. If Reclamation finds a Contractor employee to be unsuitable or unfit for his or her assigned duties, the CO

will direct the Contractor to remove the individual from the contract and access to the Federal facility at which the contract activities are occurring.

(3) The Contractor's employees governed by this contract may need access to sensitive information and/or sensitive areas. The Federal Government (Government) reserves the right, in its sole discretion, to determine suitability of Contractor personnel and deny access to any sensitive information or project specific area to any personnel for any cause.

(4) The Contractor is responsible for informing and ensuring compliance by its employees with any applicable security procedures of the Government facility where work may be performed under this contract.

(5) Any Contractor employee that will have access to a Federally-controlled facility or information system will be required to have a Government-issued identification card, consisting of a Personal Identity Verification (PIV) Card, a temporary identification card, or a visitor badge. (Note: within the Department of the Interior this card is known as a DOI Access Card.) During performance of the contract, the Contractor shall keep the COR apprised of any changes in personnel, or changes in personnel access or duration, to ensure that performance is not delayed by compliance with credentialing processes.

(6) A Contractor employee will not be provided access to a Government facility or information system until a Government PIV Card, temporary identification card, or visitor identification badge has been issued to the Contractor employee. For those individuals that will be receiving a PIV Card, the Government may, at its discretion, issue a temporary identification card or visitor identification badge after the electronic background investigation forms have been received and the investigation is initiated.

(7) All Contractor employees shall access the facility via the facility's entry screening system and visibly display the Government-issued PIV Card, temporary identification card, or visitor identification badge at all times. Contractor employees must visibly wear the Government-issued identification card at all times they are on Government facilities. Contractor employees are responsible for the safekeeping of all Government-issued identification cards, whether on-site or off-site. Cards that have been lost, damaged, or stolen must be reported to the COR and DOI Access Sponsor within 24 hours. The Contractor shall return all identification cards and card keys and any other Government property and information upon completion of performance or when personnel depart permanently or for a period of 7 days or more. The Contractor may be required to turn in access control cards or identification cards on a daily basis.

(8) Misuse or loss of access control or identification cards, or failure to comply with required surrender of such cards may, at Government discretion, result in Contractor personnel being denied access to the work site, at no cost to Government. The Contractor may be charged up to \$500 for each occurrence for any required replacement of Government-issued access control or identification cards due to loss or misuse. At the end of contract performance, or when a Contractor employee is no longer working under this contract, the Contractor shall ensure that all access control and identification cards are returned to the COR.

(9) All Contractor personnel, including subcontractor personnel, with access to the work site shall be U.S. citizens or foreign individuals legally residing in, or legally admitted to, the U.S. For all non-U.S. citizens working under this contract, irrespective of length of time working on the contract, the Contractor shall provide to the COR, legible and valid copies of the individual's passport and visa (unless individual is on the Visa Waiver Program) a minimum of 14 calendar days prior to beginning work or arriving at the facility. A driver's license is not acceptable identification. In addition, a completed form I-94 shall be submitted to the COR upon the individual's arrival at the work facility and prior to beginning work.

(10) The Contractor shall report all contacts with entities, individuals, and counsel/representatives (including foreign entities and foreign nationals) who seek in any way to obtain unauthorized access to sensitive information or areas. The Contractor shall report any violations of contract provisions, laws, executive orders, regulations, and guidance to the Contracting Officer (CO). The Contractor shall report any information raising a doubt as to whether an individual's eligibility for continued employment or access to sensitive information is consistent with the interests of National Security and the Public Trust.

(11) Unsanctioned, negligent, or willful inappropriate action on the part of the Contractor (or its employees) may result in termination of the contract or removal of some Contractor employees from Reclamation facilities at no cost to the Government. These actions include, but are not limited to, exploration of a sensitive system and/or information, introduction of unauthorized and/or malicious software, inappropriate release of sensitive information, or failure to follow prescribed access control policies and/or security procedures. Failure to comply with Reclamation policies, procedures, or other published security requirements may result in termination of the contract or removal of some contracted employees from Reclamation buildings and/or facilities at no cost to the Government.

(12) All provisions of this clause shall equally apply to all subcontractors. The Contractor shall incorporate the substance of this clause in all subcontracts.

(13) These security requirements apply to all sections of this Contract including Contract Drawings and other Contract Specifications as applicable. Related documents include other general provisions of Construction or Operations and Maintenance type Contracts, including FAR clauses by reference or as amended by related documents.

(b) Information Security Requirements.

(1) Sensitive Information. The term "sensitive information" means any information which warrants a degree of protection and administrative control as defined by Reclamation or that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act. Sensitive information is generally categorized as FOR OFFICIAL USE ONLY (FOUO) information or CONTROLLED UNCLASSIFIED INFORMATION (CUI), but in some cases may include other unclassified information. (The protection of National Security information is beyond the scope of this clause. If any work on National Security information is required under this contract, it is addressed under other contract clauses.) The Contractor shall protect this type of information from unauthorized release into public domain, or to unauthorized persons, organizations, or subcontractors. Information which, either alone or in aggregate, is deemed sensitive by Reclamation shall be handled and protected in accordance with Reclamation directives and standards for identifying and safeguarding sensitive information (SLE 02-01), which is available from the COR or at <http://www.usbr.gov/recman/DandS.html#sle>.

(i) Any Government-furnished information or material does not become the property of the Contractor and may be withdrawn at any time. Upon expiration or termination of the contract, all documents released to the Contractor and any material created using data from such documents shall be returned to the COR for final disposition. Government-furnished information residing on any electronic systems (laptops, servers, desktops, media) shall be deleted from those systems using a COR-approved data erasure solution. Only with prior authorization from the CO may the Contractor retain the material. The Contractor or subcontractor shall not disclose or release the materials provided to the Contractor to any individuals of the Contractor's organization not directly engaged in providing services under the contract or that do not have a valid need-to-know. All technical data provided to the Contractor by the Government shall be protected from public or private disclosure in accordance with the markings printed

on them. All other information relating to the items to be delivered or the services to be performed under this contract shall not be disclosed by any means without prior approval of the CO. Prohibited dissemination or disclosure includes, but is not limited to: permitting access to such information by foreign nationals or by immigrant aliens who may be employed by the Contractor, publication of technical or scientific papers, advertising, disclosure to Contractor staff not investigated and deemed acceptable at the appropriate information sensitivity level, and any other public release. The Contractor shall maintain, and furnish upon request of the CO, records of the names of individuals who have access to sensitive material in its custody. All questions regarding information security, access, and control shall be referred to the COR.

(ii) The Contractor shall not release to anyone outside the Contractor's organization any sensitive, or otherwise protected information, regardless of medium in which it is contained (for example, film, tape, document, electronic), pertaining to any part of this contract or any Reclamation program or activity, unless the CO has given prior written approval. This includes, but is not limited to, news releases, marketing promotions, articles, interviews, reports, social media posts, and any other media releases. Requests for approval shall identify the specific information to be released, the medium to be used, the purpose for the release, and a description of the need-to-know. The Contractor shall submit its request to the CO ten business days before the proposed date for release. Subcontractors shall submit requests for authorization to release through the prime Contractor to the CO.

(iii) The Contractor shall notify the COR immediately when known or suspected loss/compromise of sensitive information or other documents, notes, drawings, sketches, reports, photographs, exposed film or similar information which may affect the security interests of Government has occurred. This requirement extends to employees and other personnel working on behalf of the Contractor, and expands responsibility to include prompt reporting of security issues, including observed or subsequently discovered efforts by unauthorized persons to gain unauthorized access to sensitive information.

(2) Classified Information.

(i) The disclosure of U.S. Government documents by third parties can result in damage to our national security. While this contract may not deal directly with classified information, each contractor is obligated to protect classified information pursuant to all applicable laws and to use Government information technology systems in accordance with agency procedures so that the integrity of such systems is not compromised.

(ii) Unauthorized disclosures of classified documents (whether in print, on a blog, or on websites, or other electronic or non-electronic media) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by Federal employees and contractors, until it is declassified by an appropriate U.S. Government authority. Executive Order 13526, Classified National Security Information (December 29, 2009). Section 1.1.(c) states, 'Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.' Although the Department has taken steps to prevent access to publicly disclosed classified materials from Departmental computers, it is important to understand our continuing duties and responsibilities in this regard.

(iii) Contractors (which include all employees of the contractor, as well as subcontractors and its employees performing work for the contractor) are reminded of the following obligations with respect to the treatment of classified information and the use of unclassified government information technology systems:

(v) For contracts that require access to classified information, the contractor is responsible for obtaining the required national security clearance through the Department of the Defense National Industrial Security Program Operating Manual (NISPOM). Any classified contracts will be coordinated through the Reclamation Chief Security Officer, or for IT requirements, the Bureau Chief Information Security Officer. No contractor shall access classified information unless proper clearances have been obtained and transmitted to Reclamation. For further information, refer to 443 DM 1 or DOD NISPOM 5220.22-M dated February 28, 2006 (incorporating change 2 dated May 18, 2016).

(vi) Classified information shall not be removed from official premises.

(vii) Classified information shall not be disclosed without proper authorization.

(c) Contractor Employee Suitability and Issuance of Government Identification Cards:

(1) Performance of this contract requires Contractor personnel to have a Federal Government-issued HSPD-12/FIPS-201-1 compliant Personal Identification Verification Card (PIV Card) before being allowed unsupervised access to a Federally-controlled facility or information system. An active PIV Card issued by another Federal Government agency will be accepted by Reclamation if the associated background investigation is sufficient for the work and access to facilities and information systems required under this contract, as determined solely by Reclamation. Physical access means routine, unescorted or unmonitored access to non-public areas of a Federally-controlled facility. Logical access means routine, unsupervised access to a Level 3 or 4 Federally controlled information system.

(2) At the Government's sole discretion, the Government may issue a temporary identification card or visitor identification badge, in lieu of a PIV Card, under one of the following conditions:

(i) The individual will only be associated with Reclamation for a period of 180 days or less, will not have access to sensitive information, and any access to a sensitive area or Federal-controlled information systems will be fully supervised. The 180 calendar day period begins on the first day of the individual's affiliation with Reclamation (in this case, the date that the individual's contract performance begins) and ends exactly 180 days later, regardless of the number of times the individual actually accesses a Government facility or information system.

(ii) The individual will only have sporadic access to Federal facilities and information systems; will not have access to sensitive information; and, any access to a sensitive area or Federal-controlled information system will be fully supervised.

(iii) The individual will work exclusively outdoors, will not have access to sensitive information, and any access to a sensitive area or Federal-controlled information system will be fully supervised.

(iv) In paragraphs (i) through (iii), supervised access means the individual's access to, and movement within, a facility is monitored and controlled sufficiently to prevent access to any unauthorized areas, equipment, or information; and the individual's access to an information system is monitored and controlled sufficiently to ensure appropriate use of the system and information, and to prevent access to any unauthorized systems or information. Supervision must be performed by an individual with an active Government-issued PIV Card.

(3) The Contractor shall furnish to the COR an alphabetical list of contract personnel, to include subcontractors, who will require access to a Government facility or information system. The list shall provide the full name, social security number, date of birth, place of birth, purpose or job title, and the estimated duration of access. If the Contractor believes an individual should be issued a temporary

identification card or visitor identification badge in lieu of a PIV Card based on the conditions in paragraph (4), then the Contractor must also submit a sufficient written justification as to why the specific individual or individuals will not need a PIV Card. The Contractor shall provide this information before the start of contract performance, or before the start of an individual's performance when there is a change or addition of personnel, with sufficient time to ensure that performance is not delayed by compliance with credentialing processes.

(4) Any contract employees that will be issued a temporary identification card or visitor identification badge, in lieu of a PIV Card, at the Government's sole discretion, will be subject to the following credentialing procedures: NONE

(5) Any contract employees that will be issued a PIV Card will be subject to the following credentialing procedures:

(i) The Government will initiate the e-Qip electronic background investigation process, and give the Contractor instructions for completing the background investigation and PIV Card process. As part of the PIV Card process, each Contractor employee shall be required to appear in person at a Government PIV Enrollment Station to have personal identity verification documents verified, have a photograph taken, be fingerprinted, and to pick up and activate the PIV Card when completed. The Contractor must make its personnel available at the place and time specified by the COR in order to initiate this process.

(ii) At least two weeks before start of contract performance, the Contractor must identify all contractor and subcontractor personnel who will require (insert as appropriate physical and/or logical) access for performance of work under this contract. The Contractor must make their personnel available at the place and time specified by the COR or DOI Access Card Sponsor in order to initiate screening and background investigations. The following electronic forms, or their equivalent, shall be used to initiate the credentialing process:

(a) OPM Standard Form 85 or 85P

(b) OF 306

(c) Release to Obtain Credit Information

(d) Fingerprint Card FD-258 or electronic fingerprints (local procedures may require the fingerprinting to be done at a police station; in this case, any charges are to be borne by the Contractor).

(iii) The cost of completing the above processes and submitting the above forms, including any charges for obtaining fingerprints and traveling to a Credentialing Center for card enrollment and activation, shall be borne by the Contractor. The cost of suitability and PIV-related background investigations shall be borne by Reclamation. For contracts that require a national security clearance, the cost of obtaining the national security clearance, including any associated background investigation, will be borne by the Contractor.

(iv) Contractor employees are required to complete all forms and to give, and to authorize others to give, full, frank, and truthful answers to relevant and material questions needed to reach a suitability determination. Refusal or failure to furnish or authorize provision of information may constitute grounds for denial or revocation of credentials. Government personnel may contact the Contractor personnel being investigated in person, by telephone, or in writing, and the Contractor agrees to make them available for such contact.

(v) For each Contractor employee that will be issued a PIV Card, the Government will conduct a background investigation. The tier level of background investigation for each Contractor employee will be determined by the Government based on the risk and sensitivity levels as described in Reclamation's

“Personnel Security and Suitability Directives and Standards,” SLE 01-01, which is available at <http://www.usbr.gov/recman/DandS.html#sle>. At a minimum, each Contractor employee that will be issued a PIV Card will receive a Tier 1 [previously a National Agency Check with Written Inquiries (NACI)] Background Investigation. The minimum standards which will be used in suitability determinations are contained in the DOI Departmental Manual Part 441, Chapter 5, which is available at <http://elips.doi.gov/ELIPS/DocView.aspx?id=3858>.

(vi) Each Contractor employee in a position designated as higher than Low Risk Non-Sensitive shall be reinvestigated on a periodic basis as described in Reclamation’s Personnel Security and Suitability Directives and Standards. A reinvestigation may also be initiated when the Contractor or the Government believes that a particular individual’s continued ability to meet the contract’s minimum standards is in question; or if it is determined that the position has changed and a higher level investigation is warranted.

(vii) If a Contractor employee has worked under a Federal agency contract within the past two years, and that contract required a successfully-adjudicated background investigation at the same risk level as (or higher than) this contract, further investigation may not be necessary. The Contractor shall provide the COR with documentation that supports the individual’s previous contract work and any information, including name and social security number, date of birth, and place of birth, needed for Government verification of previous background investigation.

(viii) Contractor employees who have been successfully adjudicated will be issued DOI Access Cards, which must be activated at a USAccess Credentialing Center.

(ix) If the final adjudication is unfavorable on a Contractor employee, or if Reclamation finds a Contractor employee to be unsuitable or unfit for his or her assigned duties, the CO will direct the Contractor to remove the individual from the contract and access to the Federal facility at which the contract activities are occurring. In the event of a disagreement between the Contractor and the Government concerning the suitability of a particular employee to perform work under this contract, the Government shall have the right of final determination. Determinations under this requirement are subject to the Disputes Clause. Failure of the Contractor to comply with the requirements of this clause could constitute grounds for termination for default.

(x) Reclamation will not allow a Contractor employee access to their investigation files. An individual may request, under the provisions of the Privacy Act and/or Freedom of Information Act, copies of their files from the investigative agency (Office of Personnel Management). Reclamation will not release a copy of any investigative file, in whole or part, to the Contractor or any Contractor representative.

(xi) During performance of the contract, the Contractor must keep the COR apprised of changes in personnel to ensure that performance is not delayed by compliance with credentialing processes. Cards that have been lost, damaged, or stolen must be reported to the COR and Issuing Office within 24 hours. If reissuance of expired credentials is needed, it must be coordinated through the COR.

(xii) At the end of the contract performance, or when a contractor employee is no longer working under this contract, the Contractor must ensure that all identification cards are returned to the COR.

(d) Vessel Exclusion Barriers

(1) Proof of Certification. The contractor shall, for any vessel exclusion barrier proposed for supply and/or installation under this contract, provide the contracting officer with proof of certification in accordance with ASTM Standard F2766-11 – Standard Test Method for Boat Barriers. This proof of

certification shall be provided to the contracting officer as part of any contractor proposal for the supply and/or installation of any boat barrier proposed under this contract.

(c) Site Security Requirements

(1) General Description. This section provides provisions to ensure the full security integrity of the facility and personnel working at the facility. The work of this section may involve interfaces with a number of Government security personnel, normally coordinated through the designated COR. The Contractor is responsible for ensuring that activities are accomplished in a manner that complies fully with applicable security statutes, regulations, policies, directives, and standards.

(2) Government Security Personnel. When and where applicable, personnel may be assigned to control access, secure materials or activities at the work site, or escort Contractor personnel in sensitive areas. Personnel may include: security managers, security guards, security contractors acting as agents of the Government, law enforcement personnel, or other contractors or employees. These individuals may be used to ensure the overall security and integrity of the site or building and provide controlled access. These individuals may conduct inspections of all workers, vehicles, equipment, or materials entering, or re-entering the work site. The inspection may be done visually, with walk-through and/or hand-held metal detectors, or by other means as may be deemed necessary by Reclamation.

(3) Contractor Guard Force. At the Contractor's sole discretion, and at the Contractor's own expense, with prior written Government approval, a Contractor may be authorized to hire its own guards to secure Contractor-owned equipment and/or to protect Contractor employees or subcontractors. If such a relationship is permitted, the Contractor shall be exclusively liable for all guard activities to include action or inaction of Contractor's guard personnel. The Government will not offer nor provide any indemnification. Contractor shall be solely responsible for guards at all times to include any supervision, oversight, and for the development of local guard orders and/or procedures. The Contractor shall be responsible for coordinating all guard activities with the COR and shall develop and submit to the COR, for advance approval, any guard orders and/or guard procedures.

(4) Additional Security-Related Submittals

(i) Visitor List. The Contractor shall furnish to the COR, in advance, notification of visit of any Contractor-sponsored visitor to a Government-controlled facility. This notification should be in writing and must include the purpose or nature of the visit, the full name of the visitor, and the full name and phone number of the designated sponsor who will be physically responsible for escorting the visitor for the duration of the scheduled visit.

(ii) Delivery Schedule. The Contractor shall furnish to the COR, in advance, a schedule for all deliveries. This list shall include estimated delivery date, time, nature of the materials being delivered, and – where available – the name of delivery company and type of vehicle.

(iii) Explosives Security Plan. The Contractor shall furnish to the COR for approval, in advance, an explosives security plan at any work site where explosives will be stored or used.

(5) General Provisions.

(i) General. The Contractor shall comply with the Government's site security procedures as specified, and as requested subsequent to award of Contract. Failure of the Contractor to comply with required access controls, information handling procedures, or any other security controls or procedures, may result in revocation of Contractor personnel access to the work site. The Government reserves the right to

modify or clarify security provisions of this contract based on changing political and civil circumstances, and perceived threats to personnel or the facility.

(ii) Security Facilities and Equipment. The Contractor shall use security facilities and equipment only for the purposes intended and as directed by the CO. The Contractor shall comply with the Government's instructions for use of secure storage areas, site enclosure and gates, temporary security lighting, building space enclosure, and lockup devices and systems established for detection, monitoring, signaling, and alarming field office facilities. Measures necessary to secure the integrity of materials, equipment, and tools installed or used in furtherance of this contract shall be at no cost to the Government.

(iii) Security Personnel Availability/Work Schedules. The Contractor shall notify the COR at least 24 hours in advance of any projected work which might impact on security or require the scheduling of extended security personnel support. The Contractor shall provide a weekly work schedule, such as anticipated delivery of materials, use of explosives or heavy machinery, and extra time needed for continuous or inherently lengthy construction or project specific operations (such as concrete placement).

(iv) Deliveries. The Contractor shall provide at least one day's advance notice of major deliveries, including time of arrival and trucks/carriers/documentation to be expected for arrival at work site. The Contractor shall provide reasonable advanced notice of deliveries which must be accommodated/accepted at times other than the Government's established working hours. Failure to provide adequate advanced notice may result in delivery delays at the Contractor's expense.

(v) Site Access. All Contractor personnel will be issued appropriate identification and must comply with all local access control procedures. The Government reserves the exclusive right to refuse or disallow any vehicular or pedestrian access to any Government-controlled facility or for any deliveries to the work site, regardless if access was scheduled or unscheduled.

(vi) Inspections and Searches. The Government reserves unqualified and unlimited right at any time to conduct security-related inspections or searches of work, material, equipment, personnel, and temporary facilities at the work site. The Contractor shall afford unrestricted access to work and allow surveillance and inspection by any Government personnel as authorized by the COR. The Government reserves the right to conduct searches of articles and personal effects of all Contractor personnel, both at point of entry and exit from the work site or Government facility. All Contractor personnel entering and leaving the work site may be required to pass through a Walk-Through-Metal-Detector device and/or other detection devices.

(vii) After Duty Hours. No Contractor personnel shall be permitted access to the work site after the Government's established working hours without prior authorization from the Government. All personnel seeking access to the site after the Government's established working hours may be required to sign in and out in a visitor's log that may be maintained by the on duty security personnel (if any).

(viii) Access Procedures at Sensitive Areas. In some instances, the Contractor may be required to erect temporary security barriers and doors to isolate a sensitive area as instructed by the Government. The Contractor may be required to install locks and thereafter control access. The Contractor shall comply with the Government's requirement for limited and escorted access to the sensitive area. The Contractor shall notify the COR at least one day prior to each requested access to the sensitive area that is outside of the Government's established working hours.

(ix) Reported Violations. Where an indication, report, or observation of unauthorized access or performance of unauthorized work has occurred, the Government reserves the right to stop work and deny access until the circumstance and work can be investigated, inspected, tested, and resolved. The entire

cost of such stoppages and resolutions shall be borne by Contractor, except when alleged violations of established security requirements, after investigation, are found not to be the fault of the Contractor.

(x) Briefings. Contractor personnel who will be assigned to this project, and who will have access to the work site, may be required to attend Government-conducted security briefings. The Government reserves the right to conduct security briefings for Contractor personnel and visitors at all levels of involvement in performance of work and maintenance of security. Required briefings may include, but are not limited to, the following: Information Security, Site Security Requirements and Procedures, Delivery Methods and Inspections, Storage Requirements, Reporting Requirements, Supervisory Procedures, Contractor Employee Conduct, Visitor Control, and Threats.

(xi) Key Control. Control of keys/access codes and lock combinations is essential for the Government's project security. The Contractor shall not allow keys or access codes to be duplicated or removed from the work site, nor allow lock combinations to be divulged without specific written advanced authorization from the COR. Such loss of control, observed or suspected, may result in a requirement to change locks involved at the Contractor's expense. At the direction of the COR, the Contractor shall provide duplicate keys and lock combinations to Government security personnel when requested for the purpose of security inspections and emergency actions, including keys, combinations, and access codes needed for unrestricted access to every area and element of the project. The Contractor may be required to establish a key control program that is acceptable to the Government for Government-issued keys and for heavy machinery parked at the construction site (if this is a construction contract).

(xii) Vehicle Control. In general, parking of vehicles on the work site shall not be permitted, except for tractors, cranes, and similar equipment used directly in performance of work, for delivery of materials/supplies, and for removal of waste and surplus material. The Government may designate an approved contractor employee parking area. Upon entering the work site, vehicles and drivers may be subject to search and inspection. The Contractor shall obtain authorization from the COR to park the Contractor's official vehicles and motorized vehicular construction equipment that are required/desired to be parked on the work site. Vehicles in violation may be towed off the work site at the Contractor's expense. Where Government-designated employee parking is not available, parking of construction employees' automobiles and similar transportation vehicles may be excluded from the work site. It is the Contractor's responsibility to arrange for suitable accommodation for these vehicles.

(xiii) Prohibited/Restricted Items. Prohibited/restricted items and activities on the work site include but are not limited to the following: firearms and other weapons, except as specifically authorized by the COR in compliance with state and Federal laws and regulations; drugs, including narcotics, barbiturates, marijuana, alcoholic beverages, and similar substances, except for use with valid medical prescription; and explosives.

(xiv) Exceptions for Explosives. When needed for use in specifically limited amounts and controlled circumstances for construction work, explosives may be brought onsite with written prior authorization from the COR. As a hazardous material, the Contractor shall treat the use of explosives in accordance with regulations and guidance provided by Federal, State, and local authorities. The storage of explosives shall be in accordance with requirements of the Bureau of Alcohol, Tobacco, and Firearms or the State in which they are stored. If onsite storage of explosives is necessary, explosives shall be stored at a pre-designated, secure site approved by the COR. Prior to Government approval of storage, the Contractor shall develop and submit to the COR a complete storage/security/retrieval plan for approval. The storage/security plan can be included in a "Blasting Safety Plan." The plan shall make accommodations for surveillance, detection, and response. Explosives firing systems shall be stored off-site and under no circumstances shall be stored together with explosives.

(xv) Photography. The use of photographic equipment and taking of photographs shall only be allowed as authorized by the COR.

(f) Information Technology Security – Basic Security Requirements:

(1) The Contractor shall ensure that its employees, in performance of the contract, receive annual IT security training in Reclamation IT Security policies, procedures, computer ethics, and best practices in accordance with Reclamation Directive IRM 08-09, September 21, 2001. Subject: Reclamation Information Technology (IT) Security Program (ITSP): IT Security Awareness and Training Requirements. This document is available, upon request, from the CO. The Contractor may use web-based training available from Reclamation to meet this requirement.

(2) The Contractor shall afford Reclamation, including the Department of the Interior Office of Inspector General, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of Reclamation data or to the function of computer systems operated on behalf of Reclamation, and to preserve evidence of computer crime. If the Contractor has a question regarding the access rights or identity of Government employees requesting access to Contractor-operated IT facilities, it should be referred to the COR for resolution before access is granted.

(3) In addition to the notification requirements (b)(4), the Contractor shall immediately notify the COR, of all cyber-related incidents (including the compromise of Contractor- or Government-owned systems for which the Contractor bears operational or management responsibility), regardless of location.

52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS – COMMERCIAL ITEMS (AUG 2019)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017)(section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (JUL 2018) (Section 1634 of Pub. L. 115-91).

(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015).

(5) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(6) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004)(Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

- (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).
- (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509)
- (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (June 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)
- (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Oct 2018) (Pub. L. 109-282) (31 U.S.C. 6101 note).
- (5) [Reserved].
- (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
- (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
- (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Oct 2015) (31 U.S.C. 6101 note).
- (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).
- (10) [Reserved].
- (11)(i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011)(15 U.S.C. 657a).
- (ii) Alternate I (Nov 2011) of 52.219-3.
- (12)(i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014)(if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).
- (ii) Alternate I (Jan 2011) of 52.219-4.
- (13) [Reserved]
- (14)(i) 52.219-6, Notice of Total Small Business Set-Aside (Nov 2011)(15 U.S.C. 644).
- (ii) Alternate I (Nov 2011).
- (iii) Alternate II (Nov 2011).
- (15)(i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003)(15 U.S.C. 644).
- (ii) Alternate I (Oct 1995) of 52.219-7.
- (iii) Alternate II (Mar 2004) of 52.219-7.
- (16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).
- (17)(i) 52.219-9, Small Business Subcontracting Plan (AUG 2018)(15 U.S.C. 637(d)(4)).
- (ii) Alternate I (NOV 2016) of 52.219-9.
- (iii) Alternate II (NOV 2016) of 52.219-9.
- (iv) Alternate III (NOV 2016) of 52.219-9.
- (iv) Alternate IV (AUG 2018) of 52.219-9.
- (18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).
- (19) 52.219-14, Limitations on Subcontracting (JAN 2017) (DEVIATION 2019-O0003)(15 U.S.C. 637(a)(14)).
- (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).
- (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011)(15 U.S.C. 657 f).
- (22) 52.219-28, Post Award Small Business Program Representation (Jul 2013) (15 U.S.C. 632(a)(2)).
- (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Dec 2015)(15 U.S.C. 637(m)).
- (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Dec 2015)(15 U.S.C. 637(m)).
- (25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).
- (26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (JAN 2018) (E.O. 13126).

140R3019P0062 - Public Safety Radio Access in the Hoover Dam Security Zone
CLAUSES

- (27) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
- (28)(i) 52.222-26, Equal Opportunity (SEPT 2016) (E.O. 11246).
 - (ii) Alternate I (FEB 1999) of 52.222-26.
- (29)(i) 52.222-35, Equal Opportunity for Veterans (OCT 2015)(38 U.S.C. 4212).
 - (ii) Alternate I (JULY 2014) of 52.222-35
- (30)(i) 52.222-36, Equal Opportunity for Workers with Disabilities (JULY 2014) (29 U.S.C. 793).
 - (ii) Alternate I (JULY 2014) of 52.222-36
- (31) 52.222-37, Employment Reports on Veterans (FEB 2016) (38 U.S.C. 4212).
- (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
- (33)(i) 52.222-50, Combating Trafficking in Persons (JAN 2019) (22 U.S.C. chapter 78 and E.O. 13627).
 - (ii) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).
- (34) 52.222-54, Employment Eligibility Verification (Oct 2015). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)
- (35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA–Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
 - (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (JUN 2016)(E.O. 13693)
- (37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (JUN 2016)(E.O. 13693)
- (38)(i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).
 - (ii) Alternate I (Oct 2015) of 52.223-13.
- (39)(i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (Jun 2014) (E.O.s 13423 and 13514).
 - (ii) Alternate I (Jun 2014) of 52.223-14.
- (40) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).
- (41)(i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).
 - (ii) Alternate I (Jun 2014) of 52.223-16.
- (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (Aug 2011) (E.O. 13513).
- (43) 52.223-20, Aerosols (JUN 2016)(E.O. 13693)
- (44) 52.223-21, Foams (JUN 2016)(E.O. 13693)
- (45)(i) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).
 - (ii) Alternate I (JAN 2017) of 52.224-3.
- (46) 52.225-1, Buy American—Supplies (May 2014) (41 U.S.C. chapter 83).
- (47)(i) 52.225-3, Buy American—Free Trade Agreements—Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).
 - (ii) Alternate I (May 2014) of 52.225-3.
 - (iii) Alternate II (May 2014) of 52.225-3.
 - (iv) Alternate III (May 2014) of 52.225-3.
- (48) 52.225-5, Trade Agreements (AUG 2018) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

- (49) 52.225-13, Restrictions on Certain Foreign Purchases (JUNE 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
- (50) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
- (51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).
- (52) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).
- (53) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).
- (54) 52.232-30, Installment Payments for Commercial Items (JAN 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).
- (55) 52.232-33, Payment by Electronic Funds Transfer—System for Award Management (OCT 2018) (31 U.S.C. 3332).
- (56) 52.232-34, Payment by Electronic Funds Transfer—Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).
- (57) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).
- (58) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).
- (59) 52.242-5, Payments to Small Business Subcontractors (JAN 2017)(15 U.S.C. 637(d)(13)).
- (60)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).
 - (ii) Alternate I (Apr 2003) of 52.247-64.
 - (ii) Alternate II (FEB 2006) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

- (1) 52.222-17, Nondisplacement of Qualified Workers (May 2014)(E.O. 13495).
- (2) 52.222-41, Service Contract Labor Standards (AUG 2018) (41 U.S.C. chapter 67). *****WAGE DETERMINATION NO. 2015-5593, REVISION NO. 11, DATE OF REVISION 08/02/2019 (see Attachment 2 – Wage Determination)*****
- (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67). *****This Statement is for Information Only. It is not a Wage Determination. COMMUNICATIONS SPECIALIST; GS-11; MONETARY WAGE - \$25.78/hr; FRINGE BENEFITS – 19%, includes paid health insurance premiums, retirement benefits, vacation pay, and sick leave pay*****
- (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (AUG 2018) (29 U.S.C. 206 and 41 U.S.C. chapter 67).
- (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).
- (6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (May 2014) (41 U.S.C. chapter 67).
- (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (May 2014) (41 U.S.C. chapter 67).
- (8) 52.222-55, Minimum Wages Under Executive Order 13658 (MAR 2016)
- (9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).
- (10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (May 2014) (42 U.S.C. 1792).

(d) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records—Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (OCT 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (JUL 2018) (Section 1634 of Pub. L. 115-91).

(iv) 52.219-8, Utilization of Small Business Concerns (OCT 2018) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$700,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(v) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.

(vi) 52.222-21, Prohibition of Segregated Facilities (APR 2015)

140R3019P0062 - Public Safety Radio Access in the Hoover Dam Security Zone
CLAUSES

- (vii) 52.222-26, Equal Opportunity (SEPT 2016) (E.O. 11246).
- (viii) 52.222-35, Equal Opportunity for Veterans (OCT 2015) (38 U.S.C. 4212).
- (ix) 52.222-36, Equal Opportunity for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).
- (x) 52.222-37, Employment Reports on Veterans (FEB 2016) (38 U.S.C. 4212)
- (xi) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O.13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.
- (xii) 52.222-41, Service Contract Labor Standards AUG 2018) (41 U.S.C. chapter 67).
- (xiii) __ (A) 52.222-50, Combating Trafficking in Persons (JAN 2019) (22 U.S.C. chapter 78 and E.O 13627).
__ (B) Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O 13627).
- (xiv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (MAY 2014) (41 U.S.C. chapter 67).
- (xv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (MAY 2014) (41 U.S.C. chapter 67).
- (xvi) 52.222-54, Employment Eligibility Verification (OCT 2015) (E.O. 12989).
- (xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015).
- (xviii) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).
- (xix)(A) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).
(B) Alternate I (JAN 2017) of 52.224-3.
- (xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
- (xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792). Flowdown required in accordance with paragraph (c) of FAR clause 52.226-6.
- (xxii) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

ADDENDUM TO 52.212-5

52.204-4 PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER (MAY 2011)

(a) Definitions. As used in this clause—

“Postconsumer fiber” means— (1) Paper, paperboard, and fibrous materials from retail stores, office buildings, homes, and so forth, after they have passed through their end-usage as a consumer item, including: used corrugated boxes; old newspapers; old magazines; mixed waste paper; tabulating cards; and used cordage; or

(2) All paper, paperboard, and fibrous materials that enter and are collected from municipal solid waste; but not

(3) Fiber derived from printers’ over-runs, converters’ scrap, and over-issue publications.

(b) The Contractor is required to submit paper documents, such as offers, letters, or reports that are printed or copied double-sided on paper containing at least 30 percent postconsumer fiber, whenever practicable, when not using electronic commerce methods to submit information or data to the Government.

****END OF CLAUSES****

This page intentionally left blank

ATTACHMENT 1 – PERFORMANCE WORK STATEMENT

Public Safety Radio Service Access in the Hoover Dam Security Zone

A. INTRODUCTION.

Bureau of Reclamation (RECLAMATION), Lower Colorado Dams Office (LCDO), Hoover Dam Security Response Force (SRF) requires direct access to the Public Safety Radio Interoperability Service in the Hoover Dam Security Zone (HDSZ), in order to perform its mission to protect the facilities and the people who work at or visit the site.

B. SCOPE.

RECLAMATION requires a contractor to provide Public Safety Radio Interoperability Service ("service") in the HDSZ. The contractor shall provide "service" to the Hoover Dam SRF and to First Responders travelling to or within the HDSZ, by expanding the current coverage zone of the 800 MHz radio spectrum that is dedicated to local government public safety operations by the Federal Communications Commission (FCC). The contractor shall provide access to and useable "service" for a one-time fee. The one-time fee reimburses contractor's cost to expand Public Safety Radio Service into the HDSZ. *No additional fees will be collected for the duration of the operation and maintenance of the system on the site.*

RECLAMATION will provide a building and a tower to house the equipment, cables and antennas required to provide "service" in the HDSZ. RECLAMATION will not pay future fees for "service" because RECLAMATION provides the building, tower and utilities needed to operate the Public Safety Radio Service in the HDSZ. This includes future costs to maintain, replace or upgrade equipment or software because the contractor will own the equipment, cables, antennas and software installed on RECLAMATION's property.

Additionally, RECLAMATION will report the number of portable and vehicle radios used by SRF in the HDSZ to the Southern Nevada Communications Council (SNACC), in July of each year.

C. SITE ACCESS AND AUTHORIZATIONS.

C-1. Site Access.

Contractor personnel shall be escorted at-all-times while performing work to install or maintain "service" at Hoover Dam. The Contractor shall provide the Contracting Officer's Representative (COR) with a list of employees (names only) and vehicles (license plate numbers only) assigned to work at Hoover Dam.

C-2. Site Authorizations.

Contractor personnel shall not enter restricted areas without authorization. Restricted area entry shall be in accordance with the security regulations established for the area. Contractor shall ensure employees comply with all security rules and regulations.

Checkpoint(s) at the facility may require the contractor to allow Security to inspect and approve contractor personnel, vehicle(s), tools, materials and equipment before proceeding to their destination on-site.

Contractor parking is available at the facility. Parking shall be coordinated with the COR, in advance of arriving on-site. Certain areas may require contractor-owned vehicle keys be left inside unattended vehicles after unloading equipment.

The Contractor shall provide a Safety Plan, Tower Climb & Rescue Plan and a Schedule covering the work performed on-site. The Safety Plan and the Schedule shall be provided to the COR at least two (2)

weeks prior to commencing any on-site work (see Table 1). The submittals will be reviewed by RECLAMATION and must also be approved prior to commencing any on-site work. 70 Contractor personnel shall prepare, review and sign a Job Hazard Analysis (JHA) before beginning work on-site. The Contractor's Supervisor shall provide a signed copy of the JHA to the COR as soon as practical after signatures are obtained. A "sample" Job Hazard Analysis is available (upon request) for the Contractor's review, revision, adoption and use.

A Site Entry Permit (SEP) shall be prepared for the contractor's Job Supervisor to review and sign prior to starting work. The SEP authorizes personnel, vehicles, trailers, tools, materials, etc. to be on-site for the purpose stated. The SEP shall be released (in writing) to Reclamation upon completion of the work and removal of personnel, tools, materials, trash and waste from the facility.

Portable restrooms are available on-site for contractor personnel use. They are located at the entrance to the roadway leading up to the cell site. The Contractor may also temporarily place a portable restroom near the cell building during the construction phase of this work.

D. CELL TOWER RESTRICTIONS.

Only trained tower-climb and rescue-certified personnel shall work on the cell tower. A tower-climb and rescue-certified person plus all necessary rescue equipment must be stationed at the tower's base before climbers are allowed on the tower. Only three certified climbers shall work on the tower at the same time unless performing a rescue. The Contract Supervisor may perform rescue duties if tower-climb and rescue-certified.

E. GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, and INFORMATION.

1. RECLAMATION will provide a site, building and tower for installation of a Public Safety Radio System.
2. RECLAMATION will provide free utilities to the space housing Public Safety Radio System equipment.
3. RECLAMATION will provide an Engineering Study showing the tower can support cables and antennas required by the Public Safety Radio System.
4. RECLAMATION will provide microwave signal paths from the Hoover Dam Cell Site to Red Mountain and from Red Mountain to the BC Water Building in Boulder City, NV.
5. RECLAMATION will provide two sets of fiber interconnection points inside the BC Water Building to complete the signal path from the Hoover Dam Cell Site to the NPS Dispatch Center.
6. RECLAMATION will provide two T-1 circuits from the RECLAMATION Red Mountain building to the Red Mountain Clark County building.
7. RECLAMATION will provide and maintain portable radios carried by SRF Officers.
8. RECLAMATION will provide and maintain radios installed in SRF vehicles.

F. DELIVERABLES.

1. The Contractor will submit a schedule to install the equipment needed at Hoover Dam to provide public safety radio service to the HDSZ.
2. The Contractor will submit a schedule for testing service between multiple locations and agencies.
3. The Contractor will provide radio programming for all Hoover SRF portable and vehicle radios.
4. The Contractor will conduct multiple tests of the Public Safety Radio Service in the HDSZ to insure it is operating properly between critical radio locations (such as the Hoover Dam SRF Control Center, the NPS Dispatch Center and the Contractor's Headquarters building in Las Vegas).
5. The Contractor will test "service" between various locations in the HDSZ and the NPS Dispatch Center as requested by SRF Officers and by NPS Park Rangers.
6. The Contractor will test "service" between the NPS Dispatch Center and other Dispatch Centers in Clark County, Nevada.

7. The Contractor will test "service" between NPS Dispatch Center and First Responders travelling to or thru the HDSZ via the I-11 Bypass route and via the US Highway 93 route through Boulder City.
8. The Contractor will continue testing until the SRF Chief is satisfied the system is operating properly (a minimum of three (3) days).
9. After the System is declared operational, the Contractor will perform all maintenance required to insure components installed in the site building, on the tower, or at critical T-1 connection points (ie., Red MTN) provide reliable radio service 24 hours a day, seven (7) days a week.
10. The Contractor may invoice the one-time fee for service after NPS Dispatch declares the HDSZ Public Safety Radio System operational. *SNACC will operate and maintain the equipment at no future expense to the government into perpetuity.*
11. The Contractor will post on its website a bi-monthly report detailing airtime (in hours), total Push-To-Talk microphone keys, and total number of busies (service not available) detected by the radio system for each month in the report.

G. SUBMITTALS.

The Contractor shall furnish submittals to the Government Contracting Officer’s Representative (COR), in accordance with this paragraph, Table 1 and requirements stated in the contract. Submittals shall be interpreted to include Site Schedules, Safety Plans, Tower Climb & Rescue Plan, Job Hazard Analysis, Site Entry Permits, and a list of equipment and materials required to provide radio service.

Each submittal shall include a coversheet which references the submittal name, contract number and title and shall be provided to the COR.

Submittals may be sent via email to the COR identified following contract award.

The safety plan, tower climb & rescue plan and job hazard analysis are required submittals (see RSN 02, RSN 03, and RSN 05).

Table 1. List of Submittals

RSN	Item	Submittal Required	Due Date
01	Schedule to install equip needed to provide service in the HDSZ	Equipment installation Schedule	Two weeks before start of work on-site
02	Safety Plan for HDSZ installation	Safety Plan for HDSZ	Two weeks before start of work on-site
03	Climb and Rescue Plan to perform work on the RECLAMATION cell tower	Tower Climb/Rescue Plan for HDSZ cell tower work	Two weeks before start of work on-site
04	List of employees and vehicles assigned to work at Hoover Dam	Employee names and vehicle license plate numbers	Before work starts
05	RECLAMATION Site Work Job Hazard Analysis (JHA)	Copy of the signed Job Hazard Analysis	Before work starts
06	RECLAMATION Site Work Site Entry Permit (SEP)	Copy of the signed Site Entry Permit	Before work starts
07	Equipment & Material Lists of all items installed in the HDSZ	Equipment & Material list	Before releasing the SEP at the job's end
08	Schedule to conduct radio service tests between multiple locations and agencies	Radio Service Test Schedule	Two weeks before tests are scheduled to begin

H. PERIOD OF PERFORMANCE AND SCHEDULING.

The Contractor shall obtain and be prepared to install the equipment to provide public safety radio service in the HDSZ by February 1, 2020. (or such other date mutually agreed upon with the Contracting Office).
Note that the cell tower will be inaccessible from October 15, 2019 through January 23, 2020.

The Contractor shall provide equipment delivery dates within one month after award.

The Contractor shall provide a projected equipment installation and testing schedule for the HDSZ as soon as possible, after the equipment delivery dates are known. The installation shall not exceed 60 days after all equipment is delivered.

I. PERFORMANCE REQUIREMENTS SUMMARY (PRS).

Table 2. PRS

#	Required Performance	Performance Standard	Acceptable Performance Requirement	Method of Surveillance	Incentive
1	Radio equipment is installed & operating in the HDSZ.	Radio interoperability service is available in the HDSZ	Confirm different agency public safety radios talk to each other	observe system tests & start-up + contractor's on-line record of test results	PRS items 1 to 8 must be done to confirm radio interoperability service exists and is in service in the HDSZ. Positive or Negative past performance ratings reported to CPARS depends upon the contractor's completing the tests described in items 1 thru 8 & making the test results available in a timely manner on the contractor's website.
2	Radio service tests between three sites: SRF Control Center, NPS Dispatch, & the Contractor's Building in Las Vegas	continuous tests between these sites for three consecutive days	Confirm service exists at these three critical sites	Observe system tests, + written test results at each location	
3	Radio service tests between various HDSZ locations & NPS Dispatch	Determine if radio service exists or if the location is a null spot	Confirm service or null spot exists at these locations	Observe system tests, + written test results at each location	
4	Radio service tests between NPS Dispatch and other dispatch centers in Clark County, NV	Intermittent tests for one day	Confirm service exists between all dispatch centers		
5	Radio tests between NPS Dispatch and First Responders travelling to or thru HDSZ via I-11 Bypass route	Intermittent tests captured during the normal course of business	Confirm service exists between different agency public safety radios	observe tests as they occur + contractor's on-line record of test results	
6	Radio tests between NPS Dispatch and First Responders travelling to or thru HDSZ via US Highway 93 route	Intermittent tests captured during the normal course of business	Confirm service exists between different agency public safety radios	observe tests as they occur + contractor's on-line record of test results	

140R3019P0062 - Public Safety Radio Access in the Hoover Dam Security Zone
 ATTACHMENT 1 – PERFORMANCE WORK STATEMENT (PWS)

#	Required Performance	Performance Standard	Acceptable Performance Requirement	Method of Surveillance	Incentive
7	Continue testing until SRF Chief is satisfied the system is operating properly	Intermittent tests as requested during the normal course of business	Confirm service (or null spots) exists between the locations being tested	observe tests as they occur + contractor's on-line record of test results	<p>PRS items 1 to 8 must be done to confirm radio interoperability service exists and is in service in the HDSZ.</p> <p>Positive or Negative past performance ratings reported to CPARS depends upon the contractor's completing the tests described in items 1 thru 8 & making the test results available in a timely manner on the contractor's website.</p>
8	Testing is complete when NPS Dispatch declares (over-the-air) "HDSZ PSRS is now operational ..."	Radio interoperability service is avail in the HDSZ	Confirm different agency public safety radios talk to each other	observe system tests & start-up + contractor's on-line record of test results	
9	Bi-monthly data reports mentioned in Item F-11 above are posted on the contractor's website	Item F-11 data reports are posted as scheduled	Item F-11 data reports are available on-line within three days of the scheduled date.	Item F-11 data reports will be reviewed by the COR from the contractor's on-line website.	<p>Positive or Negative past performance ratings will be reported to CPARS depends upon timely posting of Item F-11 data reports on the contractor's on-line website.</p>

This page intentionally left blank

"REGISTER OF WAGE DETERMINATIONS UNDER | U.S. DEPARTMENT OF LABOR

THE SERVICE CONTRACT ACT | EMPLOYMENT STANDARDS ADMINISTRATION

By direction of the Secretary of Labor | WAGE AND HOUR DIVISION

WASHINGTON D.C. 20210

|

|

|

| Wage Determination No.: 2015-5593

Daniel W. Simms Division of | Revision No.: 11

Director Wage Determinations | Date Of Last Revision: 08/02/2019

Note: Under Executive Order (EO) 13658 an hourly minimum wage of \$10.60 for calendar year 2019 applies to all contracts subject to the Service Contract Act for which the contract is awarded (and any solicitation was issued) on or after January 1 2015. If this contract is covered by the EO the contractor must pay all workers in any classification listed on this wage determination at least \$10.60 per hour (or the applicable wage rate listed on this wage determination if it is higher) for all hours spent performing on the contract in calendar year 2019. The EO minimum wage rate will be adjusted annually. Additional information on contractor requirements and worker protections under the EO is available at www.dol.gov/whd/govcontracts.

State: Nevada

Area: Nevada County of Clark

****Fringe Benefits Required Follow the Occupational Listing****

OCCUPATION CODE - TITLE	FOOTNOTE	RATE
01000 - Administrative Support And Clerical Occupations		
01011 - Accounting Clerk I		15.46
01012 - Accounting Clerk II		17.36
01013 - Accounting Clerk III		19.42
01020 - Administrative Assistant		29.94
01035 - Court Reporter		26.59
01041 - Customer Service Representative I		12.51

01042 - Customer Service Representative II	14.06
01043 - Customer Service Representative III	15.34
01051 - Data Entry Operator I	13.47
01052 - Data Entry Operator II	15.23
01060 - Dispatcher Motor Vehicle	17.54
01070 - Document Preparation Clerk	15.40
01090 - Duplicating Machine Operator	15.40
01111 - General Clerk I	13.62
01112 - General Clerk II	14.85
01113 - General Clerk III	16.68
01120 - Housing Referral Assistant	20.62
01141 - Messenger Courier	13.38
01191 - Order Clerk I	15.42
01192 - Order Clerk II	16.82
01261 - Personnel Assistant (Employment) I	16.60
01262 - Personnel Assistant (Employment) II	18.57
01263 - Personnel Assistant (Employment) III	20.70
01270 - Production Control Clerk	21.01
01290 - Rental Clerk	13.53
01300 - Scheduler Maintenance	16.53
01311 - Secretary I	16.53
01312 - Secretary II	18.49
01313 - Secretary III	20.62
01320 - Service Order Dispatcher	15.67
01410 - Supply Technician	29.94
01420 - Survey Worker	15.69
01460 - Switchboard Operator/Receptionist	13.26
01531 - Travel Clerk I	16.38
01532 - Travel Clerk II	17.39
01533 - Travel Clerk III	18.66
01611 - Word Processor I	14.01
01612 - Word Processor II	15.72
01613 - Word Processor III	17.59
05000 - Automotive Service Occupations	
05005 - Automobile Body Repairer Fiberglass	25.48
05010 - Automotive Electrician	19.42
05040 - Automotive Glass Installer	18.81
05070 - Automotive Worker	18.81
05110 - Mobile Equipment Servicer	17.19
05130 - Motor Equipment Metal Mechanic	20.23
05160 - Motor Equipment Metal Worker	18.81
05190 - Motor Vehicle Mechanic	19.73
05220 - Motor Vehicle Mechanic Helper	16.39
05250 - Motor Vehicle Upholstery Worker	18.01

05280 - Motor Vehicle Wrecker	18.81
05310 - Painter Automotive	19.42
05340 - Radiator Repair Specialist	18.81
05370 - Tire Repairer	15.78
05400 - Transmission Repair Specialist	20.23
07000 - Food Preparation And Service Occupations	
07010 - Baker	16.41
07041 - Cook I	16.25
07042 - Cook II	18.04
07070 - Dishwasher	12.93
07130 - Food Service Worker	14.03
07210 - Meat Cutter	16.52
07260 - Waiter/Waitress	11.94
09000 - Furniture Maintenance And Repair Occupations	
09010 - Electrostatic Spray Painter	18.45
09040 - Furniture Handler	15.34
09080 - Furniture Refinisher	17.07
09090 - Furniture Refinisher Helper	16.15
09110 - Furniture Repairer Minor	17.74
09130 - Upholsterer	20.45
11000 - General Services And Support Occupations	
11030 - Cleaner Vehicles	10.26
11060 - Elevator Operator	14.99
11090 - Gardener	15.99
11122 - Housekeeping Aide	15.90
11150 - Janitor	15.90
11210 - Laborer Grounds Maintenance	13.25
11240 - Maid or Houseman	16.59
11260 - Pruner	12.24
11270 - Tractor Operator	15.10
11330 - Trail Maintenance Worker	13.25
11360 - Window Cleaner	17.21
12000 - Health Occupations	
12010 - Ambulance Driver	20.94
12011 - Breath Alcohol Technician	24.41
12012 - Certified Occupational Therapist Assistant	34.17
12015 - Certified Physical Therapist Assistant	33.48
12020 - Dental Assistant	17.90
12025 - Dental Hygienist	41.89
12030 - EKG Technician	32.68
12035 - Electroneurodiagnostic Technologist	32.68
12040 - Emergency Medical Technician	20.94
12071 - Licensed Practical Nurse I	21.81
12072 - Licensed Practical Nurse II	24.41

12073 - Licensed Practical Nurse III	27.21
12100 - Medical Assistant	15.59
12130 - Medical Laboratory Technician	24.11
12160 - Medical Record Clerk	17.73
12190 - Medical Record Technician	19.86
12195 - Medical Transcriptionist	17.03
12210 - Nuclear Medicine Technologist	40.21
12221 - Nursing Assistant I	11.94
12222 - Nursing Assistant II	13.43
12223 - Nursing Assistant III	14.65
12224 - Nursing Assistant IV	16.45
12235 - Optical Dispenser	22.54
12236 - Optical Technician	14.17
12250 - Pharmacy Technician	17.47
12280 - Phlebotomist	17.82
12305 - Radiologic Technologist	33.69
12311 - Registered Nurse I	28.00
12312 - Registered Nurse II	34.26
12313 - Registered Nurse II Specialist	34.26
12314 - Registered Nurse III	41.45
12315 - Registered Nurse III Anesthetist	41.45
12316 - Registered Nurse IV	49.67
12317 - Scheduler (Drug and Alcohol Testing)	30.23
12320 - Substance Abuse Treatment Counselor	23.11
13000 - Information And Arts Occupations	
13011 - Exhibits Specialist I	23.60
13012 - Exhibits Specialist II	29.25
13013 - Exhibits Specialist III	32.10
13041 - Illustrator I	24.92
13042 - Illustrator II	30.86
13043 - Illustrator III	36.78
13047 - Librarian	34.18
13050 - Library Aide/Clerk	18.06
13054 - Library Information Technology Systems Administrator	30.86
13058 - Library Technician	20.59
13061 - Media Specialist I	22.27
13062 - Media Specialist II	24.92
13063 - Media Specialist III	27.78
13071 - Photographer I	15.65
13072 - Photographer II	17.52
13073 - Photographer III	21.70
13074 - Photographer IV	26.55
13075 - Photographer V	32.11

13090 - Technical Order Library Clerk	22.69
13110 - Video Teleconference Technician	27.59
14000 - Information Technology Occupations	
14041 - Computer Operator I	17.25
14042 - Computer Operator II	19.48
14043 - Computer Operator III	21.51
14044 - Computer Operator IV	23.91
14045 - Computer Operator V	26.47
14071 - Computer Programmer I	25.73
14072 - Computer Programmer II	(see 1)
14073 - Computer Programmer III	(see 1)
14074 - Computer Programmer IV	(see 1)
14101 - Computer Systems Analyst I	(see 1)
14102 - Computer Systems Analyst II	(see 1)
14103 - Computer Systems Analyst III	(see 1)
14150 - Peripheral Equipment Operator	17.25
14160 - Personal Computer Support Technician	23.91
14170 - System Support Specialist	28.78
15000 - Instructional Occupations	
15010 - Aircrew Training Devices Instructor (Non-Rated)	29.50
15020 - Aircrew Training Devices Instructor (Rated)	35.69
15030 - Air Crew Training Devices Instructor (Pilot)	41.62
15050 - Computer Based Training Specialist / Instructor	29.50
15060 - Educational Technologist	29.80
15070 - Flight Instructor (Pilot)	41.62
15080 - Graphic Artist	24.52
15085 - Maintenance Test Pilot Fixed Jet/Prop	41.13
15086 - Maintenance Test Pilot Rotary Wing	41.13
15088 - Non-Maintenance Test/Co-Pilot	41.13
15090 - Technical Instructor	20.86
15095 - Technical Instructor/Course Developer	25.52
15110 - Test Proctor	16.84
15120 - Tutor	16.84
16000 - Laundry Dry-Cleaning Pressing And Related Occupations	
16010 - Assembler	12.87
16030 - Counter Attendant	12.87
16040 - Dry Cleaner	16.62
16070 - Finisher Flatwork Machine	12.87
16090 - Presser Hand	12.87
16110 - Presser Machine Drycleaning	12.87
16130 - Presser Machine Shirts	12.87
16160 - Presser Machine Wearing Apparel Laundry	12.87
16190 - Sewing Machine Operator	17.83
16220 - Tailor	19.07

16250 - Washer Machine	14.11
19000 - Machine Tool Operation And Repair Occupations	
19010 - Machine-Tool Operator (Tool Room)	25.79
19040 - Tool And Die Maker	30.45
21000 - Materials Handling And Packing Occupations	
21020 - Forklift Operator	18.40
21030 - Material Coordinator	21.01
21040 - Material Expediter	21.01
21050 - Material Handling Laborer	13.13
21071 - Order Filler	13.11
21080 - Production Line Worker (Food Processing)	18.40
21110 - Shipping Packer	15.83
21130 - Shipping/Receiving Clerk	15.83
21140 - Store Worker I	17.15
21150 - Stock Clerk	21.50
21210 - Tools And Parts Attendant	18.40
21410 - Warehouse Specialist	18.40
23000 - Mechanics And Maintenance And Repair Occupations	
23010 - Aerospace Structural Welder	38.07
23019 - Aircraft Logs and Records Technician	31.26
23021 - Aircraft Mechanic I	36.38
23022 - Aircraft Mechanic II	38.07
23023 - Aircraft Mechanic III	39.48
23040 - Aircraft Mechanic Helper	27.99
23050 - Aircraft Painter	34.65
23060 - Aircraft Servicer	31.26
23070 - Aircraft Survival Flight Equipment Technician	34.65
23080 - Aircraft Worker	32.90
23091 - Aircrew Life Support Equipment (ALSE) Mechanic I	32.90
23092 - Aircrew Life Support Equipment (ALSE) Mechanic II	36.38
23110 - Appliance Mechanic	24.30
23120 - Bicycle Repairer	20.53
23125 - Cable Splicer	34.12
23130 - Carpenter Maintenance	24.00
23140 - Carpet Layer	23.55
23160 - Electrician Maintenance	29.39
23181 - Electronics Technician Maintenance I	29.43
23182 - Electronics Technician Maintenance II	31.00
23183 - Electronics Technician Maintenance III	32.55
23260 - Fabric Worker	23.27
23290 - Fire Alarm System Mechanic	24.28
23310 - Fire Extinguisher Repairer	22.05

23311 - Fuel Distribution System Mechanic	25.32
23312 - Fuel Distribution System Operator	20.62
23370 - General Maintenance Worker	22.19
23380 - Ground Support Equipment Mechanic	36.38
23381 - Ground Support Equipment Servicer	31.26
23382 - Ground Support Equipment Worker	32.90
23391 - Gunsmith I	22.05
23392 - Gunsmith II	24.49
23393 - Gunsmith III	27.08
23410 - Heating Ventilation And Air-Conditioning Mechanic	25.95
23411 - Heating Ventilation And Air Contidioning Mechanic (Research Facility)	27.16
23430 - Heavy Equipment Mechanic	27.88
23440 - Heavy Equipment Operator	29.83
23460 - Instrument Mechanic	28.46
23465 - Laboratory/Shelter Mechanic	25.79
23470 - Laborer	13.13
23510 - Locksmith	23.56
23530 - Machinery Maintenance Mechanic	29.74
23550 - Machinist Maintenance	22.55
23580 - Maintenance Trades Helper	20.86
23591 - Metrology Technician I	28.46
23592 - Metrology Technician II	29.78
23593 - Metrology Technician III	30.88
23640 - Millwright	32.88
23710 - Office Appliance Repairer	20.43
23760 - Painter Maintenance	22.28
23790 - Pipefitter Maintenance	26.83
23810 - Plumber Maintenance	26.03
23820 - Pneudraulic Systems Mechanic	27.08
23850 - Rigger	31.00
23870 - Scale Mechanic	24.49
23890 - Sheet-Metal Worker Maintenance	28.32
23910 - Small Engine Mechanic	21.61
23931 - Telecommunications Mechanic I	27.85
23932 - Telecommunications Mechanic II	29.15
23950 - Telephone Lineman	22.85
23960 - Welder Combination Maintenance	24.19
23965 - Well Driller	27.08
23970 - Woodcraft Worker	27.08
23980 - Woodworker	22.05
24000 - Personal Needs Occupations	
24550 - Case Manager	16.78

24570 - Child Care Attendant	12.74
24580 - Child Care Center Clerk	17.75
24610 - Chore Aide	11.19
24620 - Family Readiness And Support Services Coordinator	16.78
24630 - Homemaker	19.78
25000 - Plant And System Operations Occupations	
25010 - Boiler Tender	32.19
25040 - Sewage Plant Operator	33.70
25070 - Stationary Engineer	32.19
25190 - Ventilation Equipment Tender	25.05
25210 - Water Treatment Plant Operator	33.70
27000 - Protective Service Occupations	
27004 - Alarm Monitor	29.99
27007 - Baggage Inspector	13.96
27008 - Corrections Officer	29.91
27010 - Court Security Officer	33.93
27030 - Detection Dog Handler	20.45
27040 - Detention Officer	29.91
27070 - Firefighter	35.43
27101 - Guard I	13.96
27102 - Guard II	20.45
27131 - Police Officer I	35.83
27132 - Police Officer II	39.81
28000 - Recreation Occupations	
28041 - Carnival Equipment Operator	12.34
28042 - Carnival Equipment Repairer	13.06
28043 - Carnival Worker	10.24
28210 - Gate Attendant/Gate Tender	17.04
28310 - Lifeguard	11.52
28350 - Park Attendant (Aide)	19.07
28510 - Recreation Aide/Health Facility Attendant	13.91
28515 - Recreation Specialist	21.93
28630 - Sports Official	15.17
28690 - Swimming Pool Operator	20.30
29000 - Stevedoring/Longshoremen Occupational Services	
29010 - Blocker And Bracer	31.92
29020 - Hatch Tender	31.92
29030 - Line Handler	31.92
29041 - Stevedore I	30.34
29042 - Stevedore II	33.62
30000 - Technical Occupations	
30010 - Air Traffic Control Specialist Center (HFO) (see 2)	39.24
30011 - Air Traffic Control Specialist Station (HFO) (see 2)	27.06

30012 - Air Traffic Control Specialist Terminal (HFO) (see 2)	29.80
30021 - Archeological Technician I	20.33
30022 - Archeological Technician II	22.74
30023 - Archeological Technician III	26.16
30030 - Cartographic Technician	28.17
30040 - Civil Engineering Technician	27.63
30051 - Cryogenic Technician I	27.11
30052 - Cryogenic Technician II	29.94
30061 - Drafter/CAD Operator I	20.33
30062 - Drafter/CAD Operator II	22.74
30063 - Drafter/CAD Operator III	25.36
30064 - Drafter/CAD Operator IV	30.87
30081 - Engineering Technician I	16.94
30082 - Engineering Technician II	19.03
30083 - Engineering Technician III	23.33
30084 - Engineering Technician IV	26.37
30085 - Engineering Technician V	32.26
30086 - Engineering Technician VI	39.04
30090 - Environmental Technician	26.42
30095 - Evidence Control Specialist	24.48
30210 - Laboratory Technician	25.49
30221 - Latent Fingerprint Technician I	31.34
30222 - Latent Fingerprint Technician II	34.61
30240 - Mathematical Technician	28.17
30361 - Paralegal/Legal Assistant I	18.47
30362 - Paralegal/Legal Assistant II	22.89
30363 - Paralegal/Legal Assistant III	28.00
30364 - Paralegal/Legal Assistant IV	33.87
30375 - Petroleum Supply Specialist	29.94
30390 - Photo-Optics Technician	28.17
30395 - Radiation Control Technician	29.94
30461 - Technical Writer I	22.46
30462 - Technical Writer II	27.49
30463 - Technical Writer III	32.96
30491 - Unexploded Ordnance (UXO) Technician I	24.94
30492 - Unexploded Ordnance (UXO) Technician II	30.17
30493 - Unexploded Ordnance (UXO) Technician III	36.17
30494 - Unexploded (UXO) Safety Escort	24.94
30495 - Unexploded (UXO) Sweep Personnel	24.94
30501 - Weather Forecaster I	28.49
30502 - Weather Forecaster II	34.64
30620 - Weather Observer Combined Upper Air Or Surface Programs	(see 2) 25.36
30621 - Weather Observer Senior	(see 2) 27.49

31000 - Transportation/Mobile Equipment Operation Occupations	
31010 - Airplane Pilot	30.17
31020 - Bus Aide	13.75
31030 - Bus Driver	17.51
31043 - Driver Courier	15.86
31260 - Parking and Lot Attendant	11.76
31290 - Shuttle Bus Driver	16.79
31310 - Taxi Driver	14.17
31361 - Truckdriver Light	16.79
31362 - Truckdriver Medium	17.72
31363 - Truckdriver Heavy	23.44
31364 - Truckdriver Tractor-Trailer	23.44
99000 - Miscellaneous Occupations	
99020 - Cabin Safety Specialist	14.71
99030 - Cashier	10.51
99050 - Desk Clerk	16.67
99095 - Embalmer	30.13
99130 - Flight Follower	24.94
99251 - Laboratory Animal Caretaker I	12.86
99252 - Laboratory Animal Caretaker II	13.61
99260 - Marketing Analyst	27.89
99310 - Mortician	30.13
99410 - Pest Controller	20.19
99510 - Photofinishing Worker	16.36
99710 - Recycling Laborer	18.58
99711 - Recycling Specialist	21.18
99730 - Refuse Collector	17.25
99810 - Sales Clerk	12.06
99820 - School Crossing Guard	15.13
99830 - Survey Party Chief	37.15
99831 - Surveying Aide	21.13
99832 - Surveying Technician	28.98
99840 - Vending Machine Attendant	18.29
99841 - Vending Machine Repairer	21.58
99842 - Vending Machine Repairer Helper	18.36

Note: Executive Order (EO) 13706 Establishing Paid Sick Leave for Federal Contractors applies to all contracts subject to the Service Contract Act for which the contract is awarded (and any solicitation was issued) on or after January 1 2017. If this contract is covered by the EO the contractor must provide employees with 1 hour of paid sick leave for every 30 hours they work up to 56 hours of paid sick leave each year. Employees must be permitted to use paid sick leave for their own illness injury or other health-related needs including preventive care; to assist a family member (or person who is like family to the employee) who is ill injured or has other health-related needs including preventive care; or for reasons resulting from or to assist a family member (or person who is like family to the employee) who is the victim of domestic violence sexual assault or stalking. Additional information on contractor requirements and worker protections under the EO is available at www.dol.gov/whd/govcontracts.

ALL OCCUPATIONS LISTED ABOVE RECEIVE THE FOLLOWING BENEFITS:

HEALTH & WELFARE: \$4.54 per hour up to 40 hours per week or \$181.60 per week or \$786.93 per month

HEALTH & WELFARE EO 13706: \$4.22 per hour up to 40 hours per week or \$168.80 per week or \$731.47 per month*

*This rate is to be used only when compensating employees for performance on an SCA-covered contract also covered by EO 13706 Establishing Paid Sick Leave for Federal Contractors. A contractor may not receive credit toward its SCA obligations for any paid sick leave provided pursuant to EO 13706.

VACATION: 2 weeks paid vacation after 1 year of service with a contractor or successor 3 weeks after 5 years and 4 weeks after 15 years. Length of service includes the whole span of continuous service with the present contractor or successor wherever employed and with the predecessor contractors in the performance of similar work at the same Federal facility. (Reg. 29 CFR 4.173)

HOLIDAYS: A minimum of ten paid holidays per year: New Year's Day Martin Luther King Jr.'s Birthday Washington's Birthday Memorial Day Independence Day Labor Day Columbus Day Veterans' Day Thanksgiving Day and Christmas Day. (A contractor may substitute for any of the named holidays another day off with pay in accordance with a plan communicated to the employees involved.) (See 29 CFR 4.174)

THE OCCUPATIONS WHICH HAVE NUMBERED FOOTNOTES IN PARENTHESES RECEIVE THE FOLLOWING:

1) COMPUTER EMPLOYEES: Under the SCA at section 8(b) this wage determination does not apply to any employee who individually qualifies as a bona fide executive administrative or professional employee as defined in 29 C.F.R. Part 541. Because most Computer System Analysts and Computer Programmers who are compensated at a rate not less than \$27.63 (or on a salary or fee basis at a rate not less than \$455 per week) an hour would likely qualify as exempt computer professionals (29 C.F.R. 541.400) wage rates may not be listed on this wage determination for all occupations within those job families. In addition because this wage determination may not list a wage rate for some or all occupations within those job families if the survey data indicates that the prevailing wage rate for the occupation equals or exceeds \$27.63 per hour conformances may be necessary for certain nonexempt employees. For example if an individual employee is nonexempt but nevertheless performs duties within the scope of one of the Computer Systems Analyst or Computer Programmer occupations for which this wage determination does not specify an SCA wage rate then the wage rate for that employee must be conformed in accordance with the conformance procedures described in the conformance note included on this wage determination.

Additionally because job titles vary widely and change quickly in the computer industry job titles are not determinative of the application of the computer professional exemption. Therefore the exemption applies only to computer employees who satisfy the compensation requirements and whose primary duty consists of:

(1) The application of systems analysis techniques and procedures including

consulting with users to determine hardware software or system functional specifications;

(2) The design development documentation analysis creation testing or modification of computer systems or programs including prototypes based on and related to user or system design specifications;

(3) The design documentation testing creation or modification of computer programs related to machine operating systems; or

(4) A combination of the aforementioned duties the performance of which requires the same level of skills. (29 C.F.R. 541.400).

2) AIR TRAFFIC CONTROLLERS AND WEATHER OBSERVERS - NIGHT PAY & SUNDAY PAY: If you work at night as part of a regular tour of duty you will earn a night differential and receive an additional 10% of basic pay for any hours worked between 6pm and 6am.

If you are a full-time employed (40 hours a week) and Sunday is part of your regularly scheduled workweek you are paid at your rate of basic pay plus a Sunday premium of 25% of your basic rate for each hour of Sunday work which is not overtime (i.e. occasional work on Sunday outside the normal tour of duty is considered overtime work).

** REQUEST FOR AUTHORIZATION OF ADDITIONAL CLASSIFICATION AND WAGE RATE Standard Form 1444 (SF-1444) **

Conformance Process:

The contracting officer shall require that any class of service employee which is not listed herein and which is to be employed under the contract (i.e. the work to be performed is not performed by any classification listed in the wage determination) be classified by the contractor so as to provide a reasonable relationship (i.e. appropriate level of skill comparison) between such unlisted classifications and the classifications listed in the wage determination (See 29 CFR 4.6(b)(2)(i)). Such conforming procedures shall be initiated by the contractor

prior to the performance of contract work by such unlisted class(es) of employees (See 29 CFR 4.6(b)(2)(ii)). The Wage and Hour Division shall make a final determination of conformed classification wage rate and/or fringe benefits which shall be paid to all employees performing in the classification from the first day of work on which contract work is performed by them in the classification. Failure to pay such unlisted employees the compensation agreed upon by the interested parties and/or fully determined by the Wage and Hour Division retroactive to the date such class of employees commenced contract work shall be a violation of the Act and this contract. (See 29 CFR 4.6(b)(2)(v)). When multiple wage determinations are included in a contract a separate SF-1444 should be prepared for each wage determination to which a class(es) is to be conformed.

The process for preparing a conformance request is as follows:

- 1) When preparing the bid the contractor identifies the need for a conformed occupation(s) and computes a proposed rate(s).

- 2) After contract award the contractor prepares a written report listing in order the proposed classification title(s) a Federal grade equivalency (FGE) for each proposed classification(s) job description(s) and rationale for proposed wage rate(s) including information regarding the agreement or disagreement of the authorized representative of the employees involved or where there is no authorized representative the employees themselves. This report should be submitted to the contracting officer no later than 30 days after such unlisted class(es) of employees performs any contract work.

- 3) The contracting officer reviews the proposed action and promptly submits a report of the action together with the agency's recommendations and pertinent information including the position of the contractor and the employees to the U.S. Department of Labor Wage and Hour Division for review (See 29 CFR 4.6(b)(2)(ii)).

- 4) Within 30 days of receipt the Wage and Hour Division approves modifies or disapproves the action via transmittal to the agency contracting officer or notifies the contracting officer that additional time will be required to process

the request.

5) The contracting officer transmits the Wage and Hour Division's decision to the contractor.

6) Each affected employee shall be furnished by the contractor with a written copy of such determination or it shall be posted as a part of the wage determination (See 29 CFR 4.6(b)(2)(iii)).

Information required by the Regulations must be submitted on SF-1444 or bond paper.

When preparing a conformance request the ""Service Contract Act Directory of Occupations"" should be used to compare job definitions to ensure that duties requested are not performed by a classification already listed in the wage determination. Remember it is not the job title but the required tasks that determine whether a class is included in an established wage determination. Conformances may not be used to artificially split combine or subdivide classifications listed in the wage determination (See 29 CFR 4.152(c)(1)).

**** HAZARDOUS PAY DIFFERENTIAL ****

An 8 percent differential is applicable to employees employed in a position that represents a high degree of hazard when working with or in close proximity to ordnance explosives and incendiary materials. This includes work such as screening blending dying mixing and pressing of sensitive ordnance explosives and pyrotechnic compositions such as lead azide black powder and photoflash powder.

All dry-house activities involving propellants or explosives. Demilitarization modification renovation demolition and maintenance operations on sensitive ordnance explosives and incendiary materials. All operations involving re-grading and cleaning of artillery ranges.

A 4 percent differential is applicable to employees employed in a position that represents a low degree of hazard when working with or in close proximity to ordnance (or employees possibly adjacent to) explosives and incendiary materials which involves potential injury such as laceration of hands face or arms of the employee engaged in the operation irritation of the skin minor burns and the like; minimal damage to immediate or adjacent work area or equipment being used. All operations involving unloading storage and hauling of ordnance explosive and incendiary ordnance material other than small arms ammunition. These differentials are only applicable to work that has been specifically designated by the agency for ordnance explosives and incendiary material differential pay.

**** UNIFORM ALLOWANCE ****

If employees are required to wear uniforms in the performance of this contract (either by the terms of the Government contract by the employer by the state or local law etc.) the cost of furnishing such uniforms and maintaining (by laundering or dry cleaning) such uniforms is an expense that may not be borne by an employee where such cost reduces the hourly rate below that required by the wage determination. The Department of Labor will accept payment in accordance with the following standards as compliance:

The contractor or subcontractor is required to furnish all employees with an adequate number of uniforms without cost or to reimburse employees for the actual cost of the uniforms. In addition where uniform cleaning and maintenance is made the responsibility of the employee all contractors and subcontractors subject to this wage determination shall (in the absence of a bona fide collective bargaining agreement providing for a different amount or the furnishing of contrary affirmative proof as to the actual cost) reimburse all employees for such cleaning and maintenance at a rate of \$3.35 per week (or \$.67 cents per day). However in those instances where the uniforms furnished are made of "wash and wear" materials may be routinely washed and dried with other personal garments and do not require any special treatment such as dry cleaning daily washing or commercial laundering in order to meet the cleanliness or appearance standards set by the terms of the Government contract by the contractor by law or by the nature of the work there is no requirement that employees be reimbursed for uniform maintenance costs.

**** SERVICE CONTRACT ACT DIRECTORY OF OCCUPATIONS ****

The duties of employees under job titles listed are those described in the
""Service Contract Act Directory of Occupations"" Fifth Edition (Revision 1)
dated September 2015 unless otherwise indicated."

Southern Nevada Area Communications Council Agenda Item

Issue: Approve the Motorola Change order 9 to include Hoover Dam ASR (Astro Site Repeater) Site and Complimentary Basic Cyber Security Risk Assessment.	Date: November 4, 2019
Petitioner: David L. Goss, SNACC Administrator	Agenda Item: 7
Recommendation - FOR POSSIBLE ACTION: That the Board approve the Motorola Change order 9 to include Hoover Dam ASR (Astro Site Repeater) Site and Complimentary Basic Cyber Security Risk Assessment and/or take action as necessary.	


Fiscal Impact:

Would reflect the same as item #6.

Background:

If the SNACC Board approves the Purchase Order for the Bureau of Reclamation to add an ASR site at the Hoover Dam, Motorola will be giving SNACC a Complimentary Basic Cyber Risk Assessment.

Respectfully Submitted:



DAVID L. GOSS

SNACC Administrator



Change Order No. 9

Date: 9/30/2019

Project Name: SNACC P-25 Migration Project – NV141108A

Customer Name: SNACC

Customer Project Mgr: David Goss

The purpose of this Change Order is to: (highlight the key reasons for this Change Order)

This change order is for the purchase and installation of the HOOVER DAM P25 SITE and the one-time complimentary demonstration of the SNACC Basic Cybersecurity Risk Assessment, as more fully described in the attached Motorola proposal dated September 25, 2019 incorporated herein by this reference.

Contract # B&Q #31428, Lease Purchase #23636

Contract Date: 12-11-2014

In accordance with the terms and conditions of the contract identified above between SNACC and Motorola Solutions, Inc., the following changes are approved:

Contract Price Adjustments

Original Contract Value:	\$18,735,778.92
Previous Change Order amounts for Change Order numbers 0 through 8	\$152,631.74
This Change Order:	\$559,335.00
New Contract Value:	\$19,447,745.66

Completion Date Adjustments

Original Completion Date:	06/15/2016
Current Completion Date prior to this Change Order:	11/30/2019
New Completion Date:	3/30/2020



Changes in Equipment: *(additions, deletions or modifications)* **Include attachments if needed**

See attached Section 3 - Equipment List in the HOOVER DAM P25 SITE proposal dated September 25, 2019.

Changes in Services: *(additions, deletions or modifications)* **Include attachments if needed**

See attached Section 7 - Warranty and Maintenance in the HOOVER DAM P25 SITE proposal dated September 25, 2019.

See attached Section 4 - Statement of Work in the HOOVER DAM P25 SITE proposal dated September 25, 2019.

This Change Order includes a one-time basic cybersecurity assessment of the SNACC Motorola radio network as detailed in APPENDIX B - Cybersecurity Assessment in the HOOVER DAM P25 SITE proposal dated September 25, 2019. No risks, corrective actions, or warranties are covered or assumed in this change order or cybersecurity assessment.

Schedule Changes: *(describe change or N/A)*

See attached Section 5 - Project Schedule in the HOOVER DAM P25 SITE proposal dated September 25, 2019.

Pricing Changes: *(describe change or N/A)*

See attached Section 8 - Pricing in the HOOVER DAM P25 SITE proposal dated September 25, 2019.

Customer Responsibilities: *(describe change or N/A)*

See attached Section 4 - Statement of Work in the HOOVER DAM P25 SITE proposal dated September 25, 2019.

Payment Schedule for this Change Order:
(describe new payment terms applicable to this change order)

25% of the Contract Price due upon change order execution (due upon effective date);
60% of the Contract Price due upon shipment of equipment;
10% of the Contract Price due upon installation of equipment; and
5% of the Contract Price due upon Final Acceptance.

Unless amended above, all other terms and conditions of the Contract shall remain in full force. If there are any inconsistencies between the provisions of this Change Order and the provisions of the Contract, the provisions of this Change Order will prevail.



IN WITNESS WHEREOF the parties have executed this Change Order as of the last date signed below.

**Motorola
Solutions, Inc.**

Customer

By: _____
Printed Name: Frank Miller
Title: Director, Systems
Integration, West Region
Date: _____

By: _____
Printed Name: _____
Title: _____
Date: _____

Reviewed by: Lauren Heise
Motorola Solutions Project Manager

Date: 9/30/2019



SOUTHERN NEVADA AREA COMMUNICATIONS COUNCIL (SNACC)

HOOVER DAM P25 SITE

SEPTEMBER 25, 2019

The design, technical, pricing, and other information ("Information") furnished with this submission is proprietary and/or trade secret information of Motorola Solutions, Inc. ("Motorola Solutions") and is submitted with the restriction that it is to be used for evaluation purposes only. To the fullest extent allowed by applicable law, the Information is not to be disclosed publicly or in any manner to anyone other than those required to evaluate the Information without the express written permission of Motorola Solutions.

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2019 Motorola Solutions, Inc. All rights reserved.

TABLE OF CONTENTS

Section 1	
System Description	1-1
1.1 Introduction	1-1
1.2 ASTRO 25 REAPTER SITE	1-1
1.2.1 Components	1-2
1.2.1.1 GTR 8000 Expandable Site Subsystem	1-2
1.2.1.2 GGM 8000 Gateway	1-2
1.2.1.3 GCP 8000 Site Controller	1-2
1.2.1.4 Radio Frequency Distribution System	1-3
1.3 Design Assumptions	1-3
1.4 backhaul requirements	1-4
Section 2	
System Drawings	2-1
Section 3	
Equipment List	3-1
Section 4	
Statement of Work	4-1
Introduction	4-1
Section 5	
Project Schedule	5-1
Section 6	
Acceptance Testing	6-3
Wide Area Trunking FDMA/TDMA Mixed Sites	6-4
Auto Site Affiliation	6-4
Talkgroup Call	6-5
Dynamic FDMA/TDMA Busy Queue Conversion	6-6
Site Trunking FDMA/TDMA Mixed Sites	6-7
Site Trunking Indication	6-7
Talkgroup Call (Single Site)	6-8
Wide Area Recovery	6-9
6.1 Signoff Certificate	6-1
Section 7	
Warranty and Maintenance	7-1
7.1 Advanced Plus Services Overview	7-1
7.2 Advanced Plus Services Description	7-1
7.2.1 Centralized Service Delivery	7-1
7.2.2 Field Service Delivery	7-2



Network Hardware Repair.....	7-2
Security Management Operations.....	7-3
Section 8	
Pricing.....	8-1
8.1 Pricing Summary.....	8-1
8.2 Post Warranty Support Estimates.....	8-1
Section 9	
Appendix A – Coverage Map.....	9-1
Section 10	
Appendix B – Cyber Security Assessment.....	10-1

SECTION 1

SYSTEM DESCRIPTION

1.1 INTRODUCTION

Motorola Solutions Inc. is proposing a new ASTRO Standalone 800MHz Repeater Site (ASR) at the Hoover Dam radio site. This ASR will be integrated into the SNACC ASTRO 25 System core assumed to be on SR 7.17 at the time of installation. The ASR site will have six channels consisting of one control channel and five voice channels. The five voice channels are equipped with TDMA operation along with Dynamic Dual Mode (DDM). DDM allows SNACC to communicate with fielded radios that are FDMA and TDMA. SNACC will need to license six new 800MHz frequencies for the Hoover Dam site.

In addition, Motorola has proposed a Cybersecurity Assessment for the SNACC ASTRO 25 Network. A Statement of Work detailing the proposed assessment is included in Appendix B.

The proposed system contains the following major components:

- One Expandable Site Subsystem (ESS) rack with six channels and two GGM 8000s
- One TX antenna – 6dBd Omni
- One RX antenna – 6dBd Omni
- One Tower Top Amp (TTA) and Control Unit Module (CMU)
- One Site Device Manager (SDM)
- One Netsure 211 DC power system – 3186 Watts with 8 hour battery backup.
- Four RAD Optimux Multiplexers (Two for Hoover Dam site and two for Red Mtn site).
- Licensing as required to add the proposed site to the SNACC network.

Redundant site links will connect the Hoover Dam site to the SNACC Core. Two existing fiber paths between the Hoover Dam site and the SNACC Red Mountain site will be utilized. Motorola has included two RAD Optimux modules at each site for interfacing each site to the existing fiber. Motorola's demarcation point at each site is the RAD multiplexer. The fiber requirements are listed in section 1.4 below. Two existing SNACC microwave paths will provide connectivity from Red Mountain to the SNACC Core.

1.2 ASTRO 25 REAPTER SITE

An ASTRO 25 Repeater Site consists of a single site with up to 28 channels and two site controllers (in a redundant configuration), which can be standalone or housed in a GTR 8000 Expandable Site Subsystem.

The GTR 8000 Expandable Site Subsystem in a repeater site is set up in a single trunked site, with one active control channel and a number of voice channels at the site. If packet data services are supported at the site, a number of voice channels can be configured with packet data channel capability. Voice traffic is routed from each of the base radios to the system for

distribution to other sites and is repeated by the base radios to support other local subscribers. However, data traffic is routed to the GCP 8000 Site Controller. The site controller routes these packets upstream to the zone controller for further processing and routing.

1.2.1 Components

The ASTRO 25 Repeater Site consists of the following components described in in further detail below.

- GTR 8000 Expandable Site Subsystem (ESS).
- GTR 8000 Repeater/Base Radio.
- GGM 8000 Site Gateway
- GCP 8000 Site Controller.
- Radio Frequency Distribution System (RFDS).

1.2.1.1 GTR 8000 Expandable Site Subsystem

The GTR 8000 Expandable Site Subsystem (ESS) enclosure can contain reconfigured GTR 8000 base stations, site LAN switches, and GCP 8000 controllers, along with an optional Radio Frequency Distribution System (RFDS), depending on your configuration needs.

Voice traffic is routed from each of the site base stations to the system for distribution all sites associated with the call. GTR 8000 Site Repeater/Base Radio

The GTR 8000 Base Radio consists of a transceiver module, power amplifier module, fan module, and power supply. The transceiver module includes the functionality for the exciter, receiver, and station control. The base radio software, configuration, and network management, as well as inbound/outbound traffic handling, are performed through this transceiver module. On-board serial and Ethernet ports are located on this module for local servicing via Configuration/Service Software (CSS).

The power amplifier module amplifies the low-level modulated RF signal from the transceiver module and delivers the amplified signal on the path to the transmit antenna. The power supply module supports the transceiver and power amplifier modules, and can also provide auxiliary power to a connected site controller or Receive Multicoupler/Low Noise Amplifier (RMC/LNA).

1.2.1.2 GGM 8000 Gateway

The GGM 8000 Gateway is a modular multi-purpose network communications platform, designed to interconnect devices and networks within ASTRO 25 public safety network systems.

The GGM 8000 provides a connection to a Wide Area Network (WAN) with no conventional channel interface (V.24, analog, and/or IP). A GGM 8000 with a connection to a WAN and with a conventional channel interface (v.24, analog, and/or IP) functions as a Site and Conventional Channel Gateway.

1.2.1.3 GCP 8000 Site Controller

The GCP 8000 Site Controller (GCP 8000) is the control interface between the transmitter/receiver subsystem and the Zone Controller. The GCP 8000 Site Controller comprises redundant site controller modules; one site controller module acts as the active



module, and the second module acts as a standby. The redundancy minimizes the possibility of a single point of failure at the site.

The GCP 8000 provides the following functions:

- Manages the channels to maximize throughput and channel availability.
- Administers registration and context activation requests.
- Monitors base stations and RF distribution equipment and interacts with the MOSCAD site device manager to facilitate centralized alarm and control monitoring.
- Provides redundant site control.
- Enables redundant site link routing for patch redundancy.

Additionally, the GCP 8000 provides the following functions at the simulcast site:

- Provides a time and frequency reference signal to the base stations, maximizing frequency stability and allowing for further site separation in a simulcast configuration.
- Provides IP simulcast capability, enabling true end-to-end IP connectivity in a simulcast configuration.

1.2.1.4 Radio Frequency Distribution System

The Radio Frequency Distribution System (RFDS) provides interconnect between the base radios and antennas, allowing for a completely contained and more compact installation footprint. For the transmitters, this can include isolators, combiners, TX filters, diplexers, and power monitors. For the receivers, this can include duplexers, site preselectors, and multicouplers. Various RFDS options exist for each of the GTR 8000 Base Radio, GTR 8000 Site Subsystem, and GTR 8000 Expandable Site Subsystem.

1.3 DESIGN ASSUMPTIONS

There were several assumptions made when designing the Hoover Dam site. The assumptions that were made are listed below:

- SNACC will coordinate and designate space to accommodate three (3) racks of equipment in accordance with proposed design documents.
- The Hoover Dam location will have adequate electrical power in the proper phase, voltage, and grounding to support the requirements of the system described.
- The total length of antenna coax between the shelter and each antenna will not exceed 450ft.
- The existing tower has space and will can support the proposed antenna system (one TX, one RX, one TTA). In accordance with proposed design documents. Coverage estimate are based on TX antenna at 120 ft and RX antenna at 140 ft.
- Spares have not been requested and have not been included.
- The connectivity between the Hoover Dam site and SNACC core is SNACC's responsibility. The demarcation point at the Hoover Dam site and Red Mountain site is the Motorola provided Optimux.



- It is assumed that there is enough bandwidth on the fiber and microwave system for Hoover Dam to be added.
- The ASR site will be 800MHz. The customer is responsible for licensing six new frequencies for the Hoover Dam site.
- A catastrophic failure of the Red Mountain site could result in a loss of both links to the Hoover Dam site and is an acceptable design limitation.

1.4 BACKHAUL REQUIREMENTS

The backhaul requirements are listed below. These requirements should be given to the carrier of the fiber network.

Backhaul specifications:

- Support QoS via Layer 2 (802.1p Priority) or Layer 3 (DSCP or ToS).
- Link Latency (one-way)—less than 70ms
- End to End Jitter—not to exceed 20 ms.
- Packet Loss— less than 0.01%.
- Bandwidth- 320 kB/s 5DS0 (T1)

Bandwidths

The bandwidths referenced are the minimums that need to be provided to ensure performance of a fully utilized site. The port speed and/or internal backhaul network may need to be greater to ensure the jitter specification is met.

Tolerance to Backhaul Network Congestion or outage

Repeater site links (including IP trunked Simulcast Prime): 2 seconds

Latency

Latency or IP Packet Transfer Delay is defined per RFC 2681

Jitter

The measurement method of jitter is based on the RFC3393 (Section 2.4) and ITU-T Recommendation Y.1541. RFC3393 specifies the calculation of the inter-packet delay variation (IPDV). ITU-T Y.1541 uses IPDV to calculate jitter. All jitter specifications are 99th percentile values. The jitter specification must apply when passing standard 1500 byte packets.

Packet Loss

This refers to "Type-P-One-Way-Packet-Loss" as defined in RFC2680, section 2.4.

In the context of audio for the ASTRO 25 network, reordered packets are also considered packet loss.

QOS Mechanisms

Four QoS levels are recommended for optimal user experience, but at least 2 are required. The following QoS mechanisms are supported:

- Layer 3 (ToS or DSCP)
- Layer 2 (802.1p Priority)

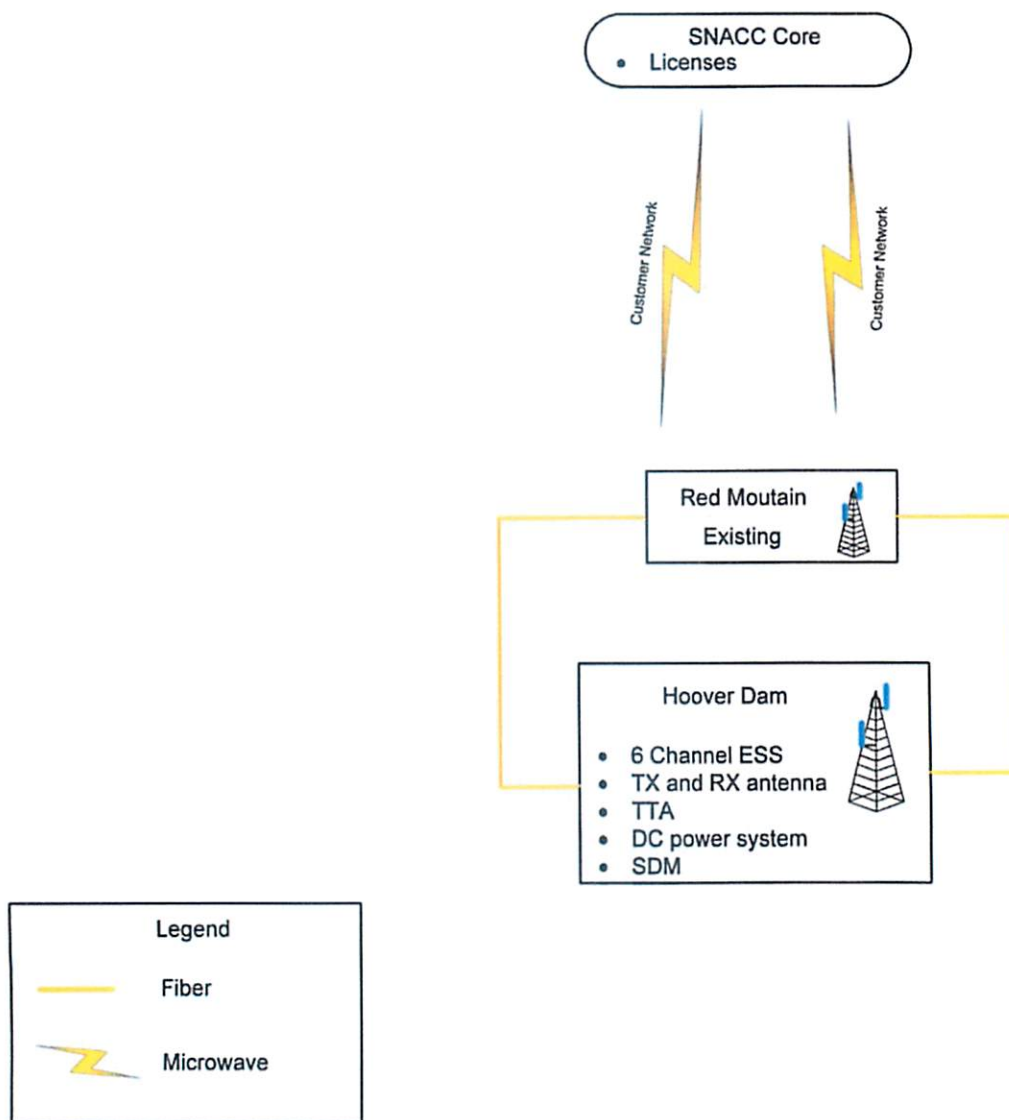
Note: If use of IPv6 on Ethernet Site/Interzone links is desired, DSCP is the required mechanism.



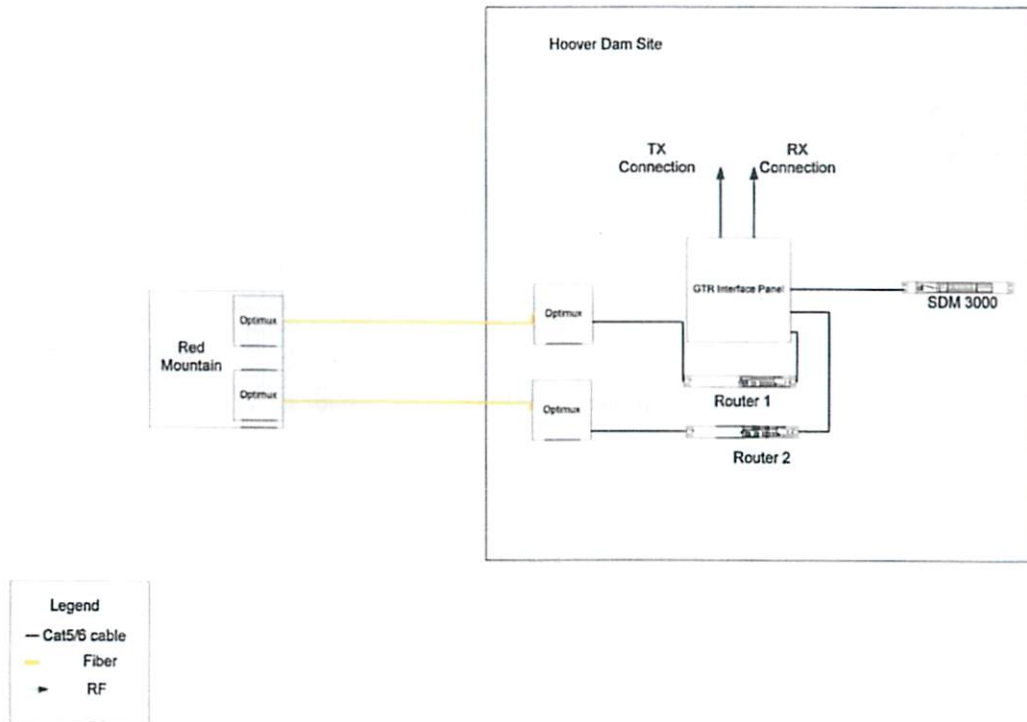
SECTION 2

SYSTEM DRAWINGS

The diagram below shows the connectivity between Hoover Dam and the SNACC Core. This diagram shows the microwave connections (the lightning bolts) and the fiber connections (the orange line).

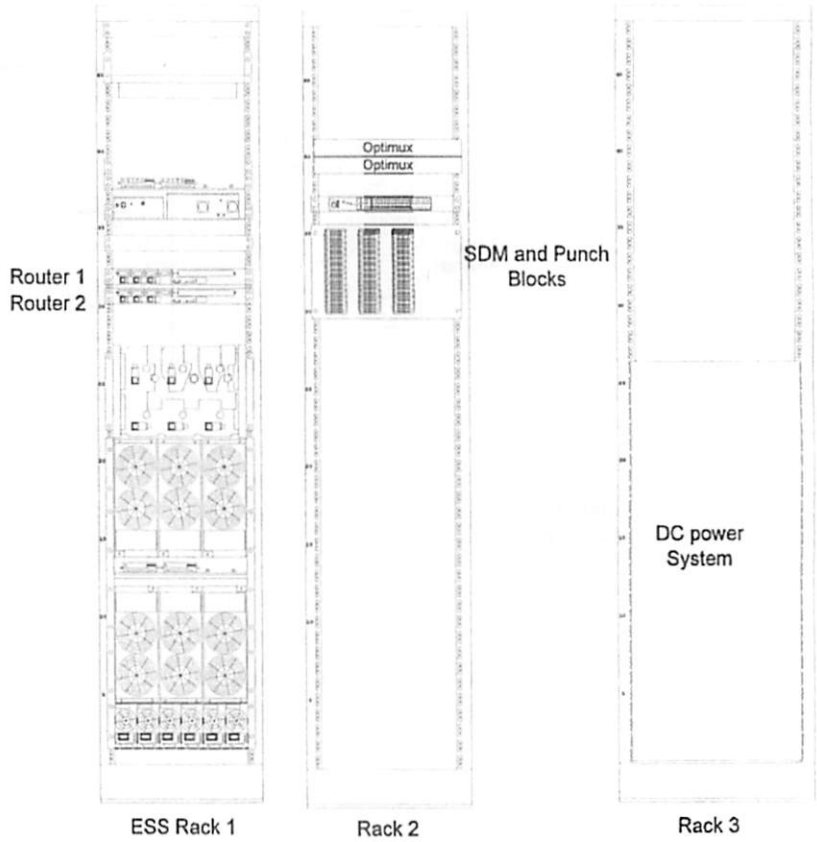


The next drawing shows the connections within the ASR site.



Below is a preliminary rack drawing for the Hoover Dam site.

- Rack 1 and 2 are 19" wide
- Rack 3 is 23" wide



SECTION 3

EQUIPMENT LIST

QTY	NOMENCLATURE	DESCRIPTION
1	SQM01SUM7054	GTR 8000 EXPANDABLE SITE SUBSYSTEM
1	CA00717AA	ADD: ASTRO SYSTEM RELEASE 7.17
1	CA00855AA	ADD: 700/800 MHZ
1	X306AC	ADD: QTY (6) GTR 8000 BASE RADIOS
5	CA01842AA	ADD: P25 TDMA SOFTWARE
5	CA01902AA	ADD: P25 DYNAMIC CHANNEL SOFTWARE
6	X591AE	ENH: ASTRO 25 SITE REPEATER SW
2	CA01706AA	ADD: ADD: GGM 8000 GATEWAY
1	CA00862AA	ADD: SITE & CABINET RMC W/CAPABILITY OF 7-24 BRS
1	CA00879AA	ADD: PRIMARY 6 PORT CAVITY COMBINER
1	CA00883AA	ADD: 800 MHZ TX FILTER W/PMU
2	CA00303AA	ADD: QTY (1) SITE CONTROLLER
2	CA02219AA	ADD: ASTRO 25 SITE REPEATER SITE CONTROLLER SOFTWARE IV&D
2	X882AH	ADD: 7.5 FT OPEN RACK, 48RU
1	CA02686AA	ADD: AC DC POWER DISTRIBUTION
1	T8343	GSERIES SOFTWARE LICENSING
6	UA00401AA	ADD: GSERIES BR-P25 TRNK ST RPTR
2	UA00406AA	ADD: GSERIES SC-P25 TRNK ST RPTR
1	DS428E83I01C48R	CONTROL MONITORING UNIT, 796-824MHZ, 16 PORT, BYPASS TEST, 48VDC REDUN
1	DS428E83I01T	TTA, NON-DIVERSITY, 796-824 MHZ, REDUNDANT LNA, TEST PORT, BYPASS
1	DSCC80706	OMNI, CORPORATE COLLINEAR, 6 DBD, 746-870 MHZ, PIM & 25 KW PIP RATED
15	L1705	LDF4-50A CABLE: 1/2" LDF HELIAX POLY JKT PER FOOT
2	DDN1090	L4TDM-PSA 7-16 DIN MALE PS FOR 1/2 IN CABLE
2	TDN9289	221213 CABLE WRAP WEATHERPROOFING
450	L3599	AVA6-50 CABLE: 1-1/4" AVA6-50, COAX CORRUG COPPER, BLACK PE JACKET
1	DS114EZDM	114EZDF DIN MALE CONNECTOR
1	DS114EZDF	114EZ DIN FEMALE CONNECTOR
8	DSSG11412B2U	SG114-12B2U 1-1/4" SUREGROUND GROUNDING KIT
3	DSL6SGRIP	L6SGRIP 1-1/4" SUPPORT HOIST GRIP
15	TDN7519	42396A-1 1-1/4" CABLE HANGER KIT STAINLESS
1	DSTSXFMBF	RF SPD, 698-2700MHZ DC BLOCK HIGH PWR, DIN FEM/MALE BI-DIR W/ BRACKET
1	DSGSAKITD	GROUND STRAP KIT - DIN
25	L1705	LDF4-50A CABLE: 1/2" LDF HELIAX POLY JKT PER FOOT
2	DDN1090	L4TDM-PSA 7-16 DIN MALE PS FOR 1/2 IN CABLE
1	DSCC80706	OMNI, CORPORATE COLLINEAR, 6 DBD, 746-870 MHZ, PIM & 25 KW PIP RATED
15	L1705	LDF4-50A CABLE: 1/2" LDF HELIAX POLY JKT PER FOOT

1	DDN1088	L4TNM-PSA TYPE N MALE PS FOR 1/2 IN CABLE
2	DDN1090	L4TDM-PSA 7-16 DIN MALE PS FOR 1/2 IN CABLE
5	TDN9289	221213 CABLE WRAP WEATHERPROOFING
5	L1705	LDF4-50A CABLE: 1/2" LDF HELIAX POLY JKT PER FOOT
1	DDN1088	L4TNM-PSA TYPE N MALE PS FOR 1/2 IN CABLE
1	DDN1090	L4TDM-PSA 7-16 DIN MALE PS FOR 1/2 IN CABLE
450	L3599	AVA6-50 CABLE: 1-1/4" AVA6-50, COAX CORRUG COPPER, BLACK PE JACKET
1	DS114EZDM	114EZDF DIN MALE CONNECTOR
1	DS114EZDF	114EZ DIN FEMALE CONNECTOR
8	DSSG11412B2U	SG114-12B2U 1-1/4" SUREGROUND GROUNDING KIT
3	DSL6SGRIP	L6SGRIP 1-1/4" SUPPORT HOIST GRIP
450	L1705	LDF4-50A CABLE: 1/2" LDF HELIAX POLY JKT PER FOOT
1	DDN1088	L4TNM-PSA TYPE N MALE PS FOR 1/2 IN CABLE
1	DDN1089	L4TNF-PSA TYPE N FEMALE PS FOR 1/2 IN CABLE
8	DSSG1212B2U	SG12-12B2U, SUREGROUND 1/2", 48"
3	DSL4SGRIP	L4SGRIP SUPPORT HOIST GRIP 1/2" LDF
15	MDN6816	STD HANGERS FOR 1/2IN CABLE & EW180/EW220/EW-HANGER KIT STAINLESS-10PK
15	TDN7519	42396A-1 1-1/4" CABLE HANGER KIT STAINLESS
1	DSTSXCDFM	RF SPD, 698 MHZ-2.7 GHZ, 60VDC PASS, DIN, MALE/FEM PIM/PIP RATED, ASIG
1	DSTSXCDFM	RF SPD, 698 MHZ-2.7 GHZ, 60VDC PASS, DIN, MALE/FEM PIM/PIP RATED, ASIG
1	DS1101378	RACK MT ADAPTER PLATE, 19 IN FOR DSOP820B, DSOP820B2 & DSNSOP820B
2	DSTSJ48CLT	SPD, RJ-45 OR HARDWIRE CONNECTED FOR T1/E1, PROTECTS 4 WIRES
1	DSTSJADP	RACK MOUNT GROUND BAR, 19 IN FOR TSJ AND WPH SERIES DATA SPD
1	DSDST20A	DISTRIBUTION PANEL (UL) W/ REAR COVER (USES PBA PLUG-IN BREAKERS)
1	DSBBA800	ISOLATED GROUND BUS BAR ASSEMBLY, 800A
1	DSOP820B	PDU, 120V HARDWIRE (8) 20A OUTLET PDU WITH TYPE 3 SAD PROTECTION
2	DSPBA10	PBA PLUG-IN BREAKER 10 AMP
4	DSPBA5	PBA PLUG-IN BREAKER 5 AMP
25	L1700	FSJ1-50A CABLE: 1/4" SUPERFLEX POLY JKT PER FOOT
2	DDN9769	F1PNM-HC 1/4" TYPE N MALE CONNECTOR FOR FSJ1-50A CABLE
25	L1702	FSJ4-50B CABLE: 1/2" SUPERFLEX POLY JKT PER FOOT
1	DDN9682	F4PNMV2-HC 1/2" TYPE N MALE PLATED CONNECTOR
1	DDN1090	L4TDM-PSA 7-16 DIN MALE PS FOR 1/2 IN CABLE
1	F4544	SITE MANAGER ADVANCED
1	VA00905	ADD:24/48 VDC PS TO SM
1	VA00872	ADD: SDM ASTRO RTU FW CURR ASTRO REL
3	V592	AAD TERM BLCK & CONN WI
1	6406066M02	PANEL PUNCH BLOCK
1	SQM01SUM0273	MASTER SITE CONFIGURATION
1	CA02629AC	ADD: EXPAND 7.17 M CORE
1	UA00153AA	ADD: ASTRO 25 FDMA SITE LICENSE



1	UA00159AA	ADD: P25 PHASE 2 TDMA TRKNG OP SITE LIC
5	UA00161AA	ADD: P25 PHASE 2 TDMA SW BASE RADIO LIC
1	UA00160AA	ADD: PHASE 2 DYNAMIC TG ASGNMT SITE LIC
5	UA00162AA	ADD: PHASE 2 DYNAMIC CH BASE RADIO LIC
4	DSS200200000 DQVERTIV20346137	OP-106-4 T1 FIBER MUX,ST,1310 NM SM SHORT HAUL
1		DC POWER SYSTEM



SECTION 4

STATEMENT OF WORK

INTRODUCTION

Motorola will install and configure the proposed equipment summarized in the attached System Description and Equipment List. The following table describes the project tasks and responsibilities involved throughout the lifecycle of the project.

Prior to starting any equipment installations, Motorola and Customer shall conduct a site readiness review examine existing work, or work performed by others, that is required to support the proposed design.

Implementation services included as part of this proposal are based on a single mobilization and will occur between normal business hours, Monday – Friday, 8:00am-5:00pm. Should SNACC require services to occur during non-business hours, additional costs may apply and will be handled via the change order process.

Project Tasks and Responsibilities

Tasks	Motorola	SNACC
Project Initiation		
Execute contract and distribute contract documents.	X	X
Assign a Project Manager as a single point of contact.	X	X
Schedule kickoff meeting.	X	
Project Administration		
Ensure that project team members attend all meetings relevant to their role on the project.	X	X
Hold regular project status meetings as agreed upon; record and distribute meeting minutes.	X	
Maintain responsibility for third-party services contracted by Motorola Solutions.	X	
Maintain responsibility for Customer's vendors and issues outside of Motorola Solutions' control.		X
Complete assigned project tasks according to the project schedule.	X	X
Submit project milestone completion document	X	
Upon completion of tasks, approve project milestone completion documents.		X
Project Kickoff / Design Review		
Introduce team, review roles, and decision authority.	X	X
Review Customer's operational requirements, project scope and objectives.	X	X
Review the Design Documents and Statement of Work.	X	X
Develop cutover plan and document final cutover process.	X	X
Develop or update mutually agreed upon detailed project schedule (Performance Schedule).	X	X
Provide heat load and power requirements for new equipment.	X	
Provide backhaul performance specifications and demarcation points.	X	
Complete the required forms required for frequency coordination and licensing.		X
Ensure that frequency availability and licensing meet project requirements, and pay licensing and frequency coordination fees.		X
Review safety, security, and site access procedure.	X	X
Update design documents, including System Description, Statement of Work, Project	X	



Tasks	Motorola	SNACC
Schedule, and Acceptance Test Plan, based on Design Review agreements		
Execute Change Order in accordance with all material changes to the Contract resulting from the Design Review.	X	X
Equipment Storage		
Provide secure warehousing.		X
Coordinate receipt of and inventory solution equipment with designated contact.	X	
Site Access		
Provide site owners/managers with written notice to provide entry to sites identified in the project design documentation.		X
Obtain site licensing and permitting, including site lease/ownership, zoning, permits, regulatory approvals, easements, power, and telco connections.		X
Site Preparation		
Provide the R56 requirements for space, power, grounding, HVAC, and connectivity requirements at each site.	X	
Ensure that each site meets the R56 standards for space, grounding, power, HVAC, and connectivity requirements.		X
Provide backhaul connectivity to meet latency, jitter and capacity requirements.		X
Verify site link performance, prior to the interconnection of the solution equipment to the link equipment.	X	
Provide adequate electrical power in proper phase and voltage at sites.		X
Provide as-built structural and foundation drawings of the structures and site locations, along with geotechnical reports, in order to facilitate a structural analysis.		X
Perform structural analysis of tower to confirm it is capable of supporting proposed antenna loads. If the tower structure fails the analysis, the cost of any site relocation or modifications to the tower required to support the antenna system will be the responsibility of SNACC.	X	
Provide cable trays, raceways, conduits, and wire supports to support wiring, cabling and coax.		X
Equipment Installation		
Deliver solution equipment to installation location.	X	
Install all proposed equipment as outlined in the System Description based upon the agreed-upon floor plans, connecting audio, control, and radio transmission cables to connect equipment to the power panels or receptacles, and audio/control line connection points. Installation performed in accordance with R56 standards and state/local codes.	X	
Bond installed equipment to the Customer provided ground system.	X	
Label installed equipment, racks, and cables.	X	
Install other equipment and subsystems not specifically listed in Motorola's equipment list and design documents.		X
Perform audit of installed equipment to ensure compliance with requirements and R56 installation standards.	X	
Antenna Equipment		
Provide and install attachment hardware for supporting transmission lines on antenna support structure.	X	
Install antennas, including supplying and installing new side arm mounts	X	
Install tower top amplifier.	X	
Install transmission lines required for system.	X	
Perform sweep tests on transmission lines.	X	
Interface and Configuration		
Provide fiber connection to demraction point at back of RAD mux at each site.		X



Tasks	Motorola	SNACC
Configure ASTRO 25 system to support the new RF site.	X	
Integrate the RF site into the system to ensure proper operation.	X	
System Optimization and Testing		
Verify that all audio and data levels are at factory specified settings.	X	
Verify communication interfaces between sites and devices for proper operation.	X	
Ensure that functionality meets manufacturers' specifications and complies with the final configuration established during design review or system.	X	
Functional Acceptance Testing		
Verify the operational functionality and features of the solution supplied by Motorola Solutions, as contracted.	X	
Witness the functional testing.		X
Document all issues that arise during the acceptance tests.	X	
If any major task for the system as contractually described fails during the Customer acceptance testing or beneficial use, repeat that particular task after Motorola determines that corrective action has been taken.	X	
Document the results of the acceptance tests and present to Customer for review.	X	
Review and approve final acceptance test results.		X
Resolve any minor task failures before Final System Acceptance.	X	
Training (not included)		
Transition to Service		
Review the items necessary for transitioning the project to service.	X	
Provide a Customer Support Plan detailing the warranty support associated with the contract equipment.	X	
Finalize Documentation		
Provide manufacturer's installation material, part list and other related material to Customer upon project completion.	X	
Provide an electronic as-built system manual on CD or other Customer preferred electronic media. The documentation will include the following: <ul style="list-style-type: none"> • Site Block Diagrams • Site Equipment Rack Configurations • ATP Test Checklists • Functional Acceptance Test Plan Test Sheets and Results • Equipment Inventory List Documentation will be delivered in Adobe PDF format on CD/DVD or USB (2 copies).	X	
Receive and approve documentation.		X
Final Acceptance		
Sign the Final Project Acceptance Certificate.	X	X

Either Party may request changes to the general scope of this Agreement. If a requested change causes an increase or decrease in the cost or a change in system configuration the Parties will agree to an equitable adjustment of the Contract Price and will reflect the adjustment in a Change Order. Neither Party is obligated to perform requested changes unless both Parties execute a written Change Order.



SECTION 5

PROJECT SCHEDULE

The estimated time for completion of the project is four to six months from Project Kickoff through Final Project Acceptance. A mutually agreed upon detailed project schedule will be developed by the Motorola Solutions' Project Manager upon contract award during the Contract Design Review (CDR) phase of the project.



SECTION 6

ACCEPTANCE TESTING

WIDE AREA TRUNKING FDMA/TDMA MIXED SITES

Auto Site Affiliation

1. DESCRIPTION

A Radio affiliation is a function that links a unique radio ID and unique talkgroup to a specific site. This information is stored in a affiliation table in the zone database.

Before resources are assigned, the affiliation table is accessed to know which sites need to be assigned to support the call. Only the sites that need to be assigned that have associated talkgroups will be assigned. If the site does not have that talkgroup affiliated to it will not be assigned. This allows for more calls to be processed with fewer resources.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 2

This test requires the ZoneWatch feature.

Note: There are system settings which could affect the assignment of resources, such as required site.

VERSION #1.030

2. TEST

- Step 1. Turn RADIO-1 off and on.
- Step 2. Verify via ZoneWatch that RADIO-1 sends in its affiliation.
- Step 3. Initiate a call using RADIO-1 on TALKGROUP 1.
- Step 4. Verify RADIO-2 can receive and respond to the call. Using ZoneWatch verify that no resources are assigned at SITE 2 as there are no subscribers affiliated to TALKGROUP 1 at SITE 2.
- Step 5. Initiate a call on TALKGROUP 2 using RADIO-3.
- Step 6. Verify that RADIO-4 can receive and respond to the call. Using ZoneWatch verify that no resources are assigned at SITE 1 as there are no subscribers affiliated to TALKGROUP 2 at SITE 1.

Pass____ Fail____

Wide Area Trunking FDMA/TDMA Mixed Sites

Talkgroup Call

1. DESCRIPTION

The Talkgroup is the primary level of organization for communications on a trunked radio system. Radios with Talkgroup call capability will be able to communicate with other members of the same Talkgroup. This provides the effect of a private channel down to the Talkgroup level. This test will demonstrate that a Talkgroup transmission initiated by a radio user will only be heard by system users, which have, the same Talkgroup selected. As with other types of calls, Talkgroup calls can take place from anywhere in the system.

SETUP

RADIO-1 - SITE 1 - TALKGROUP 1
RADIO-2 - SITE 2 - TALKGROUP 1
RADIO-3 - SITE 1 - TALKGROUP 2
RADIO-4 - SITE 2 - TALKGROUP 2

VERSION #1.040

2. TEST

- Step 1. Initiate a Wide Area Call with RADIO-1 in TALKGROUP 1.
- Step 2. Observe that only RADIO-2 will be able to monitor and respond to the call.
- Step 3. Initiate a Wide Area Call with RADIO-3 in TALKGROUP 2.
- Step 4. Observe that only RADIO-4 will be able to monitor and respond the call.

Pass____ Fail____

Wide Area Trunking FDMA/TDMA Mixed Sites

Dynamic FDMA/TDMA Busy Queue Conversion

1. DESCRIPTION

If no voice channel resources are available, radios requesting channels for new conversations are placed in a queue. Users of the same priority will move through the queue in a FIFO (first in, first out) sequence.

When a voice channel becomes available, the radio at the top of the busy queue gets a channel assignment and generates a callback tone if the FDMA/TDMA mode of the call can be supported by the available resource. While the call is waiting in the busy queue, the FDMA/TDMA mode of a talkgroup at a site in site trunking can be change as radios join or leave the talkgroup.

NOTE: All radios and talkgroups should start with default priorities. The Default is 10.

SETUP

RADIO-1 (TDMA) - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 (TDMA) - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-8 (FDMA-only) - TALKGROUP 2
RADIO-8 - SITE - SITE 1
RADIO-9 (FDMA-only) - TALKGROUP 2
RADIO-9 - SITE - SITE 1

VERSION #1.010

2. TEST

- Step 1. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 2. Initiate a TALKGROUP 2 call using RADIO-9. Verify RADIO-8 receives the call. Keep the call in progress until instructed to end it. Observe that the channel is assigned in the FDMA mode.
- Step 3. Initiate a TALKGROUP 1 call using RADIO-1 and observe that the radio receives a busy.
- Step 4. Dekey RADIO-9 and observe that RADIO-1 receives a callback and can make the call. Observe that the channel is assigned in the TDMA mode since there are no FDMA-only radios in the call.
- Step 5. Initiate a TALKGROUP 2 call using RADIO-9 and observe that the radio receives a busy.
- Step 6. Dekey RADIO-1 and observe that RADIO-9 receives a callback and can make the call. Observe that the channel is assigned in the FDMA mode.

Pass____ Fail____

SITE TRUNKING FDMA/TDMA MIXED SITES

Site Trunking Indication

1. DESCRIPTION

When a remote site loses its link or does not have a link to the Zone Controller, the affected site will enter "Site Trunking" mode of operation. Radios locked onto this site will be serviced locally within this site's coverage area.

NOTE: If the subscriber does not have the Display option, the "Site Trunking" indication will not be displayed.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1

Lock the subscribers to SITE 1 if more than one site exists on the system.

VERSION #1.010

2. TEST

- Step 1. Place SITE 1 into the Site Trunking mode.
- Step 2. Verify that RADIO-1 and RADIO-2 are displaying the "Site Trunking" indication.
- Step 3. Return the site to Wide Area Trunking unless the next test requires Site Trunking.

Pass _____ Fail _____

Site Trunking FDMA/TDMA Mixed Sites

Talkgroup Call (Single Site)

1. DESCRIPTION

When a site goes into Site Trunking, radios with Talkgroup Call capability will be able to communicate with other members of the same talkgroup at that same site. (Members of the same talkgroup at other sites will not be able to monitor those conversations.)

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 1

* All Radios should be "Site Locked"

VERSION #1.010

2. TEST

- Step 1. Place SITE 1 into the Site Trunking mode.
- Step 2. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1 at SITE 1.
- Step 3. Observe that only RADIO-2 will be able to monitor and respond to the call. Note that RADIO-3 AND RADIO-4 are not able to monitor the call since they are on another Talkgroup.
- Step 4. Initiate a Talkgroup Call with RADIO-3 on TALKGROUP 2 at SITE 1.
- Step 5. Observe that only RADIO-4 will be able to monitor and respond to the call.
- Step 6. Return the site to Wide Area Trunking unless the next test requires Site Trunking.

Pass____ Fail____

Site Trunking FDMA/TDMA Mixed Sites

Wide Area Recovery

1. DESCRIPTION

A site in Site Trunking will transition to Wide Area Trunking when all failures have been cleared. All subscribers should transition from Site Trunking to Wide Area Trunking and continue to process calls.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 1
RADIO-4 - SITE - SITE 2
CONSOLE-1 - TALKGROUP 1

Note: All Radios should be "Site Locked"

VERSION #1.020

2. TEST

- Step 1. Set the status of SITE 1 to Wide Area and clear any system errors that may have placed SITE 1 into Site Trunking.
- Step 2. Verify that the status of SITE 1 has transitioned into Wide Area Trunking.
- Step 3. Verify that RADIO-1 and RADIO-2 no longer display Site Trunking.
- Step 4. Verify Wide Area communications between RADIO-1, RADIO-2, RADIO-3, RADIO-4 and CONSOLE-1.

Pass ____ Fail ____

6.1 SIGNOFF CERTIFICATE

By their signatures below, the following witnesses certify they have observed the system Acceptance Test Procedures.

Signatures

WITNESS: _____ Date: _____

Please Print Name: _____

Please Print Title: _____

Initials: _____

SECTION 7

WARRANTY AND MAINTENANCE

Motorola Solutions will provide warranty services per our standard warranty terms and conditions as outlined within the existing Agreement, B&Q #31428, Lease Purchase #23636. In addition to the warranty services, Motorola Solutions has included our Advanced Plus Services package to commence with and run concurrently with the Warranty Period.

7.1 ADVANCED PLUS SERVICES OVERVIEW

Advanced Plus Services focuses on monitoring the network on an ongoing basis, proactively mitigating potential functionality and security issues, and providing both remote and onsite support. The proposed offering consists of the following specific services:

- Service Desk.
- Technical Support.
- Network Event Monitoring.
- Onsite Support.
- Annual Preventative Maintenance.
- Network Hardware Repair with Advanced Replacement.
- Remote Security Patch Installation.
- Network Updates.

These services will be delivered through the combination of local service personnel either dedicated to the network or engaged as needed; a centralized team within Motorola's Solutions Support Center (SSC), which operates on a 24 x 7 x 365 basis; and our Repair Depot, which will ensure that equipment is repaired to the highest quality standards. The collaboration between these service resources, all of who are experienced in the maintenance of mission-critical networks, will enable a swift analysis of any network issues, an accurate diagnosis of root causes, and a timely resolution and return to normal network operation.

7.2 ADVANCED PLUS SERVICES DESCRIPTION

7.2.1 Centralized Service Delivery

Centralized support will be provided by Motorola's support staff, located at our Service Desk and Solutions Support Center (SSC). These experienced personnel will provide direct service and technical support through a combination of Service Desk telephone support, technical consultation and troubleshooting through the SSC, and ongoing network monitoring of the system.

Motorola will provide **Service Desk** response as a single point of contact for all support issues, including communications between SNACC, third-party subcontractors and manufacturers, and

Motorola. When personnel call for support, the Service Desk will record, track, and update all Service Requests, Change Requests, Dispatch Requests, and Service Incidents using Motorola's Customer Relationship Management (CRM) system. The Service Desk is responsible for documenting inquiries, requests, concerns, and related tickets; tracking and resolving issues; and ensuring timely communications with all stakeholders based on the nature of the incident.

As tickets are opened by the Service Desk, issues that require specific technical expertise and support will be routed to our Solutions Support Center (SSC) system technologists for **Technical Support**, who will provide telephone consultation and troubleshooting capabilities to diagnose and resolve infrastructure performance and operational issues. Motorola's recording, escalating, and reporting process applies ISO 90001 and TL 9000-certified standards to the Technical Support calls from our contracted customers, reflecting our focus on maintaining mission-critical communications for the users of our systems.

The same SSC staff that provide direct telephone support will also provide **Network Event Monitoring** to your network in real-time, ensuring continuous management of the system's operational functionality. The SSC's technicians will utilize sophisticated tools to remotely monitor the system, often identifying and resolving anomalous events before they might affect user communications.

7.2.2 Field Service Delivery

Onsite repairs and network preventative maintenance will be provided by authorized local field services delivery personnel, who will be dispatched from and managed by the Solutions Support Center.

OnSite Support provides local, trained and qualified technicians who will arrive at your location upon a dispatch service call to diagnose and restore the communications network. This involves running diagnostics on the hardware or FRU (Field Replacement Unit) in order to identify defective elements, and replacing those elements with functioning ones. The system technician will respond to the location in order to remedy equipment issues based on the impact of the issue to overall system function.

Annual Preventive Maintenance Service provides proactive, regularly scheduled operational testing and alignment of infrastructure and network components to ensure that they continually meet original manufacturer specifications. Certified field technicians perform hands-on examination and diagnostics of network equipment on a routine and prescribed basis.

Network Hardware Repair

Network Hardware Repair – Motorola's authorized Repair Depot will repair the equipment provided by Motorola, as well as select third-party infrastructure equipment supplied as part of the proposed solution. The Repair Depot will manage the logistics of equipment repair (including shipment and return of repaired equipment), repair Motorola equipment, and coordinate the repair of third-party solution components.

Motorola also proposes **Network Hardware Repair with Advanced Replacement**. With this additional service, Motorola will exchange malfunctioning components and equipment with advanced replacement units or Field Replacement Units (FRUs) as they are available in the Repair Depot's inventory. Malfunctioning equipment will be evaluated and repaired by the infrastructure repair depot and returned to the Repair Depot's FRU inventory upon repair



completion. If customers prefer to maintain their existing FRU inventory, a "loaner" FRU can be requested while a unit is being repaired.

Security Management Operations

The proposed **Remote Security Patch Installation Service** will provide you with pre-tested security updates, pre-tested and remotely installed by Motorola on your system. When appropriate, Motorola will make these updates available to outside vendors in order to enable them to test each patch, and will incorporate the results of those third-party tests into the updates before installation on your network. Once an update is fully tested and ready for deployment in your system, Motorola will remotely install it onto the system, and notify you that the patch has been successfully installed. If there are any recommended configuration changes, warnings, or workarounds, Motorola will provide detailed documentation along with the updates on the website.



SECTION 8

PRICING

8.1 PRICING SUMMARY

Description	Price
Equipment and Services Total	\$658,041.00
Discount for Purchase of Entire System as Proposed	-\$32,902.00
Discount for Executed Contract by October 16, 2019	-\$65,804.00
TOTAL	\$559,335.00

8.2 POST WARRANTY SUPPORT ESTIMATES

The below pricing is for information only and will be added to the existing support agreement per the terms of the agreement.

	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8
Maintenance	\$16,492.00	16,986.76	\$17,496.36	\$18,021.25	\$18,561.89	\$19,118.75	\$19,692.31
SUA II	\$8,399.51	\$8,404.51	\$8,410.51	\$8,415.51	\$8,421.51	\$8,426.51	\$8,432.51
Total	\$24,891.51	\$25,391.27	\$25,906.87	\$26,436.77	\$26,983.40	\$27,545.26	\$28,124.82

SECTION 9

APPENDIX A – COVERAGE MAP

The following coverage maps are based on assumed parameters and are for informational purposes only. Coverage verification testing or coverage acceptance testing are not included in the proposed project. The first map shows just the Hoover Dam ASR site and the second is a composite of all the current sites plus the Hoover Dam site. The dark blue in the maps represent the portable inbound coverage and the green represents the portable outbound coverage.

- Informational coverage assumptions:
 - Portable Used:
 - APX 6000
 - Swivel case with mic
 - 5 Watts of power
 - GTR8000
 - GTR ESS
 - 40 Watts of power





SNACC System
Hoover Dam Add

This map is a coverage estimate based upon currently known details and should be used for informational purposes only. This coverage estimate in no way constitutes a coverage guarantee and Motorola is not responsible for any deviation between the estimated and actual system performance.



0 4 8 16 Miles
1 inch = 6.31 miles
Projection: GCS_North_American_1983
Sources: Esri, HERE, DeLorme, USGS, Intermap, INCREMENT P, NRCan, Esri Japan, METI, Esri China (Hong Kong), Esri Korea, Esri (Thailand), Mapbox, NGCC, OpenStreetMap contributors, and the Open User Community

SECTION 10

APPENIX B – CYBER SECURITY ASSESSMENT





MOTOROLA SOLUTIONS

**Cybersecurity Risk Assessment
Statement of Work
Southern Nevada Area Communications
Council (SNACC)**

Version 1.0

September 2019

VERSION AND CHANGE CONTROL

Revision History

Version	Revision Date	Revised By	Change Description
1.0	25 Sep 2019	Cybersecurity Offer Management	Creation

This Statement of Work (SOW), including all of its subsections and attachments is an integral part of the Professional Services Agreement or other signed agreement between Motorola Solutions, Inc. ("Motorola") and Customer ("Agreement") and is subject to the terms and conditions set forth in the Agreement.

SERVICE OVERVIEW

Cyber attacks have the ability to dramatically impact the confidentiality, integrity and availability of your operation. It is critical that holistic assessment is conducted to identify cyber risk and implement a strategy which maximizes security and increases your cybersecurity risk posture. Through this service, Motorola Solutions will:

- Deploy cybersecurity professionals to holistically assess Motorola Solutions provided technology within the customer operation in full alignment with the National Institute of Technology and Standards (NIST) cybersecurity framework. As part of the pre-engagement phase of the assessment, the full scope of the customer operation for assessment will be agreed upon between Motorola Solutions and the customer.
- Generate a cybersecurity assessment report and accompanying presentation which displays assessment findings. The report will also include prioritized risk assessment of findings.
- Provide a cybersecurity remediation plan which addresses the findings of the assessment.
- Provide a remediation report which summarizes the work recommended to be carried out within the remediation phase.

It is the outcome focussed objective of this service to increase the cyber resilience of the customer operation. This requires not only detailed risk assessment but also professional services consultancy to implement remediation in order to reduce risk.

CYBERSECURITY ASSESSMENT PROPOSED SCOPE AND ACTIVITIES

Motorola Solutions' cybersecurity risk assessment is split into 3 phases. The phases are displayed in the table below along with associated sub tasks. Detailed description of sub tasks are covered in this document

Pre-Engagement	On-Site Assessment	Post-Assessment
Engagement Kickoff	Customer Interviews	Analysis and Reporting
Planning & Preparation	NIST Aligned Risk Assessment	Presentation of Findings
Engagement Scope Confirmation		Remediation Plan

PRE-ENGAGEMENT

Engagement Kickoff

The Engagement kickoff is the first meeting to begin the cybersecurity risk assessment process. In this phase, Motorola Solutions cybersecurity services representatives will meet with the appropriate personnel from the customer organization to discuss the upcoming engagement. Subjects are not limited to but will include the following topics in order to obtain as much information prior to the on-site assessment:

- Introductions
 - Introduction to Motorola Solutions and customer personnel who will be involved in the cybersecurity risk assessment engagement
 - Overview of the process and next steps
- Customer Operation Overview
 - High level understanding of the customer operation
 - Technologies in use within the customer operation
 - Existing network diagrams and system architecture
 - Operation objectives and critical system components
 - Geographical locations
- Existing customer approach to cybersecurity
 - Current organizational roles and responsibilities
 - Current security policies and procedures

- Examination of any previous security assessments which have taken place
- Understanding of any cybersecurity concerns over any specific areas of the operation
- Proposed dates for the on-site assessment
- Next Steps
 - Following the engagement kick off, Motorola Solutions will require a period of reasonable time to digest all of the information gathered and provide engagement scope confirmation for customers agreement

Engagement Scope Confirmation

Motorola Solutions will arrange a subsequent call with the customer to provide a detailed proposal for the scope of the cybersecurity risk assessment engagement. Motorola Solutions will also provide details of the post-assessment remediation recommendations and consultancy services which are included in this engagement.

It is a requirement of this service engagement that agreement is obtained and the customer assessment permission form is signed by the customer.

ON-SITE ASSESSMENT

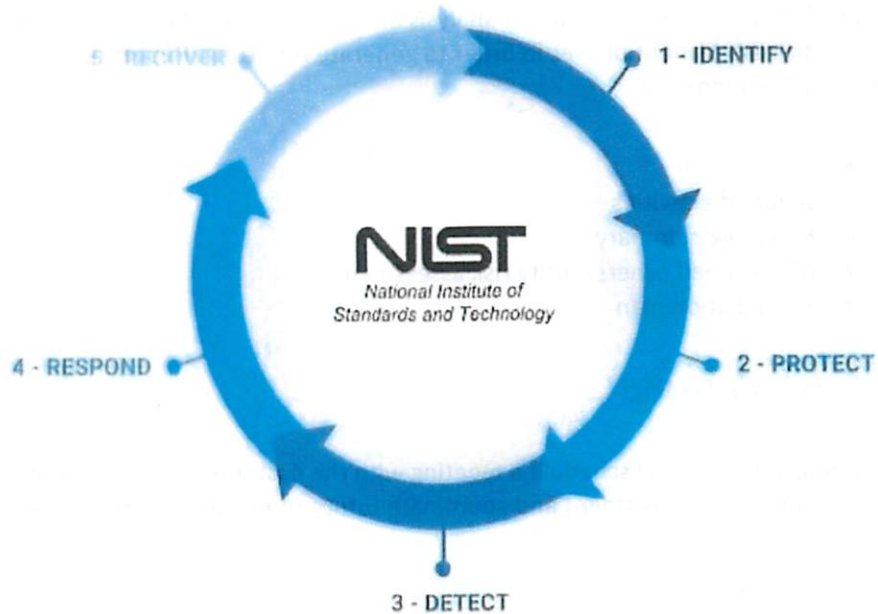
Customer Interviews

Once on site, Motorola Solutions will conduct a series of interviews with pre-arranged personnel to greater understand the day to day operations of the customer environment. The intended interviews and objectives, if applicable to the customer operation will aim to include but not limited to:

Role	Objective of the Interview
IT Director / Chief Information Security Officer (CISO)	Understanding of the management approach to cybersecurity within the operation
IT Security Manager / IT Manager	Understanding of the day to day operational practices and procedures of the customer environment
System Operator / End User	Understanding of how the security policies and practices flow down from management to the system operators and end users

NIST Aligned Cybersecurity Risk Assessment

Motorola Solutions will conduct a NIST aligned cybersecurity risk assessment against system scope as agreed within the engagement scope confirmation phase.



A detailed list of all NIST cybersecurity framework controls which will be applied to the customer operation can be found at Appendix A of this document

POST-ASSESSMENT

Analysis and Reporting

Motorola Solutions will conduct an analysis of all data collected during the pre-engagement and on-site assessment phases in order to generate reporting. Reporting will include the following components:

- Introduction
- Scope of activities
- Executive summary
- NIST aligned cybersecurity risk assessment
- Remediation plan

Presentation of Findings

Motorola Solutions will schedule a meeting with the customer to present the findings of the cybersecurity risk assessment and coordinate future remediation steps.

Remediation Plan

Motorola Solutions will provide a remediation plan which is specifically tailored to the findings of the cybersecurity risk assessment, prioritized by risk rating.

ROLES AND RESPONSIBILITIES

Motorola Responsibilities

- a. **Project Lead.** Motorola Solutions will assign a project lead to oversee the engagement, interface with customer's project management team and provide project status as needed during the assessment.
- b. **Experienced and Senior Security Professional.** Motorola Solutions will provide one Cybersecurity subject matter expert who will:
 - i. Conduct a kick-off meeting with the customer to identify the scope of the assessment.
 - ii. Conduct the on-site elements of the assessment with the assistance of the customer's technical point of contact.
 - iii. Conduct an off-site analysis of the data collected and generate the final report. Motorola will provide one (1) hard copy and one (1) PDF electronic copy of the report to the customer.
 - iv. Create a final summary presentation of the results and conduct a review of the assessment results with the customer. Motorola will provide one (1) hard copy and one (1) PDF electronic copy of the presentation to the customer.
- c. **Recommended Assessment Sites/Locations.** All site locations must be within a 20 mile radius of the zone core or additional charges will be assessed. Motorola Solutions resources will perform a physical inspection and technical evaluation of up to 2 locations comprised of the following types of sites:
 - i. A minimum of 1 (One) Zone Core location
 - ii. A minimum of 2 (Two) RF and Microwave Site locations
 - iii. A minimum of 2 (Two) Dispatch Site locations

Motorola Solutions may perform inspections and technical evaluations of additional sites if they can be completed within the time allotted for the site visit
- d. **Deliverables.** Motorola Solutions shall provide the following deliverables as an output of the assessment activity:
 - i. **Cybersecurity assessment report and accompanying presentation** - The report and accompanying presentation outlines the findings of the cybersecurity assessment and provides an overview of the cybersecurity risk posture
 - ii. **Cybersecurity remediation plan** - The remediation plan is a recommendation on how the remediation professional services consultancy can be best utilized. This is to be discussed with the customer and agreed upon prior to commencing the remediation professional services consultancy

- iii. **Remediation Report** - A report which summarizes the work carried out within the remediation professional services consultancy phase

Customer Responsibilities

- a. **Confirmation of Scope.** Customer will receive and must acknowledge in writing the Cybersecurity Professional Service Statement of Work provided by Motorola prior to initiating the service.
- b. **Kickoff Support.** Customer must participate in the kickoff meeting, which identifies the scope of the assessment.
- c. **Contacts.** Customer must appoint at least one (1) primary contact (customer project manager) and one (1) technical point of contact that are trained and knowledgeable of the project objectives to assist Motorola's project lead and Motorola's security specialist and answer any technical or business process questions. Customer's partners, consultants or any third parties involved in the project shall likewise provide access to their resources, and shall not restrict access by Motorola to customer resources.
- d. **Reasonable Access to Resources.** Customer must provide reasonable access to necessary resources as requested by the project manager, including access to the applicable facilities, network equipment and systems. Where access directly by the Motorola engineer is not permissible, customer must provide the necessary technical expertise to acquire the necessary data or information for Motorola.
- e. **Reasonable Access to Information.** Customer must provide Motorola with reasonable access to any information necessary to facilitate the project. Such requests may include site plans, facility layout, network topography or other documentation. Where access directly by the Motorola engineer is not permissible, customer must provide the necessary technical expertise to acquire the necessary data or information for Motorola.
- f. **Site Conditions.** Customer will ensure that all work sites it provides will be safe, secure, and in compliance with all applicable industry and OSHA standards.
- g. **Customer Review.** Customer will review project documentation as it is received to provide feedback for appropriate and timely discussions and/or changes.
- h. **On-Site Assessment.** Customer and Motorola will agree on the dates and times associated with Motorola's on-site activities. Customer will provide the necessary access and resources, as described above, throughout those periods.
- i. **Access to Work Space, Telephone and Internet.** Customer must provide access to work space, telephone and Internet connectivity to Motorola during the project. This access will be used solely for purposes of project execution.
- j. **Physical Access On Site.** Customer must provide any escort, badges, security personnel, labor resources or other necessary assistance to enable Motorola's access

to required work areas on site. Customer is responsible for all costs associated with availability and use of these resources.

- k. **Third-Party Equipment, Software and Services.** Unless specifically provided by Motorola's service delivery team described herein, customer is responsible for all third-party services, equipment and software associated with this service.
- l. **Project Changes.** Customer must communicate schedule changes for tasks or phase events to the Motorola project manager. Customer understands such changes may lead to additional costs for which the customer would be responsible.

Limitations and Restrictions

- a. Motorola Solutions Cybersecurity risk assessment will be performed on standard Motorola workdays, Monday–Friday, 8am to 5pm, unless otherwise negotiated. After-hours work can be performed at an additional cost.
- b. The service does not include optimization of equipment.
- c. This service does not include provisioning of security service overlays (PENTEST, 2-Factor Authentication, Compliance Management, Implementation Services, etc.)
- d. The on-site component of this service requires a minimum of two weeks advance notice for scheduling the on-site engagement.
- e. If Motorola is unable to complete the on-site data gathering portion due to equipment malfunction or unavailability/access, (including customer designated point(s) of contact) customer may be responsible for any additional time and travel charge for subsequent attempts to obtain the needed data to satisfactorily complete the assessment.

Appendix A

NIST Cybersecurity Framework Core Controls

IDENTIFY (ID)	<p>Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.</p>	<p>ID.AM-1: Physical devices and systems within the organization are inventoried</p>
		<p>ID.AM-2: Software platforms and applications within the organization are inventoried</p>
		<p>ID.AM-3: Organizational communication and data flows are mapped</p>
		<p>ID.AM-4: External information systems are catalogued</p>
		<p>ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value</p>
		<p>ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established</p>
	<p>Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to</p>	<p>ID.BE-1: The organization’s role in the supply chain is identified and communicated</p>

	<p>inform cybersecurity roles, responsibilities, and risk management decisions.</p>	<p>ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated</p>
		<p>ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated</p>
		<p>ID.BE-4: Dependencies and critical functions for delivery of critical services are established</p>
		<p>ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)</p>
	<p>Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.</p>	<p>ID.GV-1: Organizational cybersecurity policy is established and communicated</p>
		<p>ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners</p>
		<p>ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed</p>
		<p>ID.GV-4: Governance and risk management processes address cybersecurity risks</p>
	<p>Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>ID.RA-1: Asset vulnerabilities are identified and documented</p>
		<p>ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources</p>

		ID.RA-3: Threats, both internal and external, are identified and documented
		ID.RA-4: Potential business impacts and likelihoods are identified
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		ID.RA-6: Risk responses are identified and prioritized
<p>Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>		ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed
		ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
<p>Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.</p>		ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
		ID.SC-2: Suppliers and third party partners of information systems, components, and

		<p>services are identified, prioritized, and assessed using a cyber supply chain risk assessment process</p>
		<p>ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.</p>
		<p>ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.</p>
		<p>ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers</p>
<p>PROTECT (PR)</p>	<p>Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</p>	<p>PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes</p>
		<p>PR.AC-2: Physical access to assets is managed and protected</p>
		<p>PR.AC-3: Remote access is managed</p>
		<p>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties</p>

	<p>PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)</p>
	<p>PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions</p>
	<p>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)</p>
<p>Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	<p>PR.AT-1: All users are informed and trained</p>
	<p>PR.AT-2: Privileged users understand their roles and responsibilities</p>
	<p>PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities</p>
	<p>PR.AT-4: Senior executives understand their roles and responsibilities</p>

		<p>PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities</p>
		<p>PR.DS-1: Data-at-rest is protected</p>
		<p>PR.DS-2: Data-in-transit is protected</p>
		<p>PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition</p>
	<p>Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p>PR.DS-4: Adequate capacity to ensure availability is maintained</p>
		<p>PR.DS-5: Protections against data leaks are implemented</p>
		<p>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity</p>
		<p>PR.DS-7: The development and testing environment(s) are separate from the production environment</p>

			PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
	<p>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
			PR.IP-2: A System Development Life Cycle to manage systems is implemented
			PR.IP-3: Configuration change control processes are in place
			PR.IP-4: Backups of information are conducted, maintained, and tested
			PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
			PR.IP-6: Data is destroyed according to policy
	PR.IP-7: Protection processes are improved		

	PR.IP-8: Effectiveness of protection technologies is shared
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
	PR.IP-10: Response and recovery plans are tested
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
	PR.IP-12: A vulnerability management plan is developed and implemented
<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
<p>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

			<p>PR.PT-2: Removable media is protected and its use restricted according to policy</p>
			<p>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities</p>
			<p>PR.PT-4: Communications and control networks are protected</p>
			<p>PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations</p>
<p>DETECT (DE)</p>	<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	<p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed</p>	
		<p>DE.AE-2: Detected events are analyzed to understand attack targets and methods</p>	
		<p>DE.AE-3: Event data are collected and correlated from multiple sources and sensors</p>	
		<p>DE.AE-4: Impact of events is determined</p>	

		<p>DE.AE-5: Incident alert thresholds are established</p>
<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>		<p>DE.CM-1: The network is monitored to detect potential cybersecurity events</p>
		<p>DE.CM-2: The physical environment is monitored to detect potential cybersecurity events</p>
		<p>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events</p>
		<p>DE.CM-4: Malicious code is detected</p>
		<p>DE.CM-5: Unauthorized mobile code is detected</p>
		<p>DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events</p>
		<p>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed</p>

		DE.CM-8: Vulnerability scans are performed
	<p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
		DE.DP-2: Detection activities comply with all applicable requirements
		DE.DP-3: Detection processes are tested
		DE.DP-4: Event detection information is communicated
		DE.DP-5: Detection processes are continuously improved
RESPOND (RS)	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	RS.RP-1: Response plan is executed during or after an incident
	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	RS.CO-1: Personnel know their roles and order of operations when a response is needed

		<p>RS.CO-2: Incidents are reported consistent with established criteria</p>
		<p>RS.CO-3: Information is shared consistent with response plans</p>
		<p>RS.CO-4: Coordination with stakeholders occurs consistent with response plans</p>
		<p>RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness</p>
	<p>Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.</p>	<p>RS.AN-1: Notifications from detection systems are investigated</p>
		<p>RS.AN-2: The impact of the incident is understood</p>
		<p>RS.AN-3: Forensics are performed</p>
		<p>RS.AN-4: Incidents are categorized consistent with response plans</p>

		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-1: Incidents are contained
		RS.MI-2: Incidents are mitigated
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned
		RS.IM-2: Response strategies are updated
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned
		RC.IM-2: Recovery strategies are updated
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g.	RC.CO-1: Public relations are managed

	coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	RC.CO-2: Reputation is repaired after an incident
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

Appendix B

RISK MANAGEMENT METHODOLOGY

Risk Level

The overall risk level of the particular risk is calculated by likelihood and impact. This field enables sorting and prioritization of the risks within the register. The 5x5 risk rating matrix visualizes the relationship between likelihood and impact. There are four possible risk ratings (Low, Medium, High, Extreme):

Risk Rating Matrix	Impact				
	Minor	Moderate	Major	Severe	Catastrophic
Likelihood					
Almost Certain	Medium (7)	High (14)	Extreme (20)	Extreme (22)	Extreme (25)
Likely	Medium (6)	High (13)	High (16)	Extreme (21)	Extreme (24)
Possible	Low (4)	Medium (9)	High (15)	High (18)	Extreme (23)
Unlikely	Low (2)	Medium (8)	Medium (10)	High (17)	High (19)
Rare	Low (1)	Low (3)	Low (5)	Medium (11)	Medium (12)

Within the risk rating matrix above, "Likelihood" is on the Y axis, and "Impact" is on the X axis. Once a risk is assigned both a likelihood and an impact rating, it is automatically assigned an overall risk level based on where the selection of those two variables places the risk within the risk rating matrix.

The numbers within each cell in the Risk Rating matrix (1-25) allow the ranking and prioritization of risks even if they fall within the same general risk rating categories (Low, Medium, High, Extreme).

