1) I would like to know the project budget or estimate for RFP-DEM-12-13-015 Facility Security System Replacement.

A: There is no set budget for this project; however price does play a factor in the award selection.

2) Are you expecting the winning bid provider to issue “a nationally approved FIPS 201 PIV /First Responder Authentication Credential (FRAC) card?” via a card issuing service?

A: This will be done onsite using customer equipment. We will not accept a card issuing service.

3) If the answer is no, which PIV-I / FRAC Issuer will be used?

A: This specific project is for a PIV interoperable credentialing that meets FIPS. We will be our own issuer.

4) Will the FIPS 201 PIV / FRAC card support a Card Authentication Key (CAK)?

A: Yes. This is a requirement.

5) Can you elaborate on what you mean by a Primary FRAC Database? We are not familiar with this type of database. Is this a database that is provided by the US Government?

A: A FRAC database is similar to a “cardholder” database, but it contains the full number of fields for Personal Identity Verification as defined by US Federal Information Processing Standard 201 for Personal Identity Verification – Interoperable (PIV-I) credentials. “Middleware” software that brings a specific vendor’s cardholder database up to compliance with FIPS-201 PIV-I standards is acceptable, but such middleware and all associated costs must be included in the proposal.

6) Can you elaborate on what you mean by validation of the FRAC credential? Is this validation of the applicant before the FRAC is issued? If so, which validation methodologies must be used? Or is this validation of the FRAC after it has been issued to ensure it has not been cloned or fraudulently created by using the Authentication PKI Certificate?

A: “Validation” refers to an access control event where a proximity or contact smart chip card is presented at a reader. Specifically, when a FRAC credential is presented at a reader, the credential should be validated against its related
authentication factors in the cardholder database and/or the Cardholder Unique Identifier Key stored in the credential’s smart chip as referenced in http://www.idmanagement.gov/documents/PIV-I_FAQ.pdf.

7) Will strong authentication at the door be implemented at certain entry points? Which ones?

A: All doors will have two-tier strong authentication, with the exception of all exterior doors at Facility “A” and “C” will have three tier strong authentication.

8) Who will be the Certificate Authority?

A: The vendor must specify whether the proposed solution is capable of locally verifying a certificate generated by the proposed hardware and software solution (i.e. the customer will be acting as its own certificate issuing authority) or if the proposed solution requires the use of an external certificate issuing authority (i.e. failure of the customer to use an external certificate issuing authority would result in reduced system capabilities). As a reminder, we are not requesting the ability to interface with Federal issuing authorities in this RFP.

9) What is the memory storage capacity on the card?

A: ISO 7816 is the internationally accepted standard for smart cards. ISO 7816 is a family of standards primarily dealing with aspects of smart card interoperability regarding communication characteristics, physical properties, and application identifiers of the implanted chip and data.

<table>
<thead>
<tr>
<th>CARD: ACOS1 – 8k</th>
<th>RAM CAPACITY: 10 MB</th>
<th>EPROM STORAGE: 8KB</th>
<th>Triple DES, Authentication, 8 byte PIN</th>
</tr>
</thead>
</table>

10) How many Open Options door licenses and or sub controllers licenses does the division currently own?

A: The Division owns 1 “client” license, 0 “badging” licenses, 1 “driver” license, and 10 “subcontroller” licenses.

11) Would DEM consider switching out the entire system?

A: Yes, we would consider it if it is cost effective to the State and not proprietary.

12) Does your current license include Way Point or Open DX?

A: No.

13) What is your reader count vs. door count?
A: Facility A, 8 doors and 2 non-door readers; Facility B, 4 exterior doors and 4 interior doors readers; Facility C, 5 doors with 5 readers.

14) Are current readers HID compliant?

A: There are several disparate access control systems across the facilities. This RFP is for total replacement of all system components, and as stated in the RFP, all readers in the vendor’s proposed solution must be HID compliant readers that meet FIPS 201 PIV standards.

15) How many doors are being controlled by Open Options?

A: Two.

16) Do all proximity readers need to be able to also read a contact smart reader?

A: Yes, all proximity readers must include a contact smart chip reader; they must also include either a pin pad or pin pad plus biometric reader based on the specifications of the RFP.

17) Clarification and questions about supply of uninterrupted power.

A: The State is responsible for supplying uninterruptable power, where needed. Responses must include the physical location and power requirements for all system components requiring independent electrical supply (non-PoE).

18) Describe the current DEM Network and bandwidth.

A: The State recognizes that the performance of many system components, configurations, and features may depend on particular network addressing techniques, such as multicast, which are not enabled or are discouraged on current DEM networks. Likewise, it is recognized that current bandwidth availability may be sub-optimal for certain security system components or configurations. The State is not averse to making modifications to the existing DEM network if, in the State’s sole judgment, the advantages to be gained justify collateral effort or expense. In order for this to be accurately evaluated, responses must include the network requirements (PoE, bandwidth, multicast) for each component or connection, a diagram of proposed device interconnectivity, and WAN requirements (bandwidth, multicast) for remote equipment (Facility C). For any proposed new video equipment, the response must indicate whether or not DSCP can be enabled and set.

19) Will Facility C require real time video? If yes, will it require new cameras?

A: Specific to the security cameras, facility C must have real-time video capabilities on the local equipment and network inside facility C, which is currently accomplished with the existing Panasonic DVR, monitors, and control stations. Given the extensive network needs for live video, the Division is
comfortable with using the existing DVR web application to view these cameras across its network in Facilities A and B on an as-needed basis.

Specific to the intercoms, video from the intercoms should be viewable real-time during an intercom call only when the scheduling on door stations routes the call to master stations in Facility A.

20) Please clarify the 1 hour response requirement?

A: Upon further internal discussion, this requirement is defined as follows: A service technician from the vendor must verbally acknowledge the maintenance request within 1 hour. For critical issues as defined in the answer to question #34, physical response of a service technician at the affected facility must occur within 4 hours of verbally acknowledging the request.

21) Will there be an attendee list provided?

A: No. You may request a copy of the attendance list after award.

22) Will you provide drawings to the facilities before we submit a proposal?

A: Drawings of the facilities will not be provided due to the secure nature of the facilities. However, we have provided the number of doors and types of readers. Drawings of the facilities will be provided to the awarded vendor.

23) Will we have a time to post technical questions regarding site C?

A: Addendum #2 allowed time for additional questions.

24) Can we just up the licensing for the current card program you are using?

A: No, the current card making software is proprietary to Digital Data Research Company and is not compatible with OpenOptions. If the vendor proposes reuse of our existing OpenOptions environment, then they will need to propose a replacement badge making solution that is both compatible with OpenOptions, generates our FRAC card format, and stores all FIPS-201 PIV fields in the cardholder database.

25) Do you already have licensing available for the amount of kiosk you will be using? Will these also need to interface with the badging system based on the different types that were outlined during the walk through?

A: All current badging systems and visitor management kiosks will be replaced. The division does not currently own any OpenOptions Waypoint visitor kiosk licenses. As stated in the RFQ, visitor badges created on the visitor system must be capable of being temporarily assigned access rights for one or many doors to the facility. We recognize that this integration may require the issuance of a
visitor card with an RFID chip and are willing to pair a blank RFID card with a paper label and/or plain PVC visitor card as needed.

26) If we use the current Data card systems with the existing software, could you outline the standard so we can use it with compatible readers? Could we have the specs for the sp-75 and sp-55 card types that will be used on the project?

A: We wish to REPLACE the current card software as well as the cards. The SP-75 Plus and SP-55 model numbers refer only to the existing card printers that will be used. Their specifications can be obtained from the Datacard Group website.

27) The cat 6 cabling specifications were outlined based on the facilities could these different wiring standards be used? I.e. what color schemes are needed based on which building. Example: all new cat 6 might be blue, black if used for networking, red for the intercom systems etc.

A: The cabling referred to must be CAT6, in addition to meeting all other applicable requirements of codes or common industry standards appropriate to the installation parameters. Cable colors, in buildings A & B, should be red for access components, green for video components, orange for intercom components, yellow for audio components. In Building C: green for access components, red for video components, orange for intercom components, purple for audio components. It should noted that if a color conflict with existing cable is discovered during installation, an alternate color will be selected by the customer.

28) There are different types of card readers, do they require all factors of authentication or will this vary by group. Example: one reader ask for long range RFID, smart chip, proximity+pin+ biometric. Will that mean that the user will have to use their RFID, the card reader on contact, a pin + the biometric fingerprint? Will this be outlined in the questions regarding which group requires which authentication method? If not all authentication methods?

A: The intention of specifying contact smart chip and proximity in every reader is to ensure future compatibility and the capability for credentials issued by other authorities to be read by our system. Proximity OR contact smart chip should be considered as one factor, (i.e. only one or the other needs to be presented at the reader). The remaining factor(s) for validation will be pin pad for all interior readers and pin pad plus biometric for the exterior readers on facilities “A” and “C.”

29) How many users will need to access the camera and camera movements at a time? How many will just need to see the camera stationary?

A: Facility A and B should be on the same control system, which needs to have a minimum of 2 locations to view + control cameras and two additional locations to
view cameras. The ability to have additional login sessions viewing and/or controlling cameras from inside the customer's network through a web browser based app is highly desirable. Facility C will need to have a minimum of 2 locations to view + control cameras.

30) What is meant by 9/1 ceiling mounted speakers and 7+2 /7 Wall mounted horn style speakers, can you elaborate or provide examples?

A: Please see clarification below.

IP Addressable and powered Public Address speakers for facility A and B:

- 10 ceiling-mounted speakers for office suites, lobbies, and large rooms.
- 16 wall-mounted “horn” style speakers for open cubicle areas and hallways
- If PoE is used, devices must include a power injector if needed for the specific location. In addition to meeting any other required specifications, all wiring intended as a network connection shall be to CAT6 specifications. The contractor will be required to supply any necessary new patch panels and they shall meet customer’s current conventions.
- All installation locations are within 250 feet of the nearest network closet.

IP Addressable and powered Public Address speakers for facility C:

- 6 ceiling-mounted speakers for office suites, lobbies, and large rooms.
- 12 “horn” style speakers for open cubicle areas, storage space and warehouse areas.
- If PoE is used, devices must include a power injector if needed for the specific location. In addition to meeting any other required specifications, all wiring intended as a network connection shall be to CAT6 specifications. The contractor will be required to supply any necessary new patch panels and they shall meet customer’s current conventions.
- All ceiling-mounted speakers are within 250 feet of the network closet. Horn-style speakers designated for open warehouse areas may be located up to 1500 feet away from the network closet.

Optional PA Systems shall be addressable from certain intercom master stations (if IP-based and interfaced with intercom system) or hand held microphones with PTT button and wall mounting clip (if configured on local amplifiers) as follows:

Facility “B”: 4 locations
Facility “C”: 6 locations

If separate amplifiers are needed, each facility shall be on its own separate PA amplifier and local to that facility.

31) Can the local 1 hr. maintenance for un correctable emergency situations be sub contracted locally by an authorized dealer?

A: Yes; note that the 1 hour requirement was clarified in question #20
32) Does licensing count as an open platform for hardware? I.e. if you want to add a camera company and you do so for a small fee is this applicable in this scenario?

A: The Division’s interpretation of an “Open Platform” is a platform that allows other vendors of competing yet interrelated products (ex. access control software, cardholder database applications and middleware, security cameras, card readers, door controllers, system boards, etc) to freely and openly develop application program interfaces between the competing products so that a customer can achieve the greatest unification of products for a comprehensive security system. If the proposed solution includes licensing fees for the disparate products that the vendor is quoting for a comprehensive solution, those costs must be disclosed (including whether the licensing fees are one-time or annual) and will be weighed as part of the selection process.

33) For the intercom and camera solutions with Aiphones did you want those to record 180 days for the intercom as well or were these an entirely standalone system?

A: They should be an entirely standalone system in regard to the intercom audio and video portion. Any storage of video/audio events on the Aiphone intercoms should be limited to base configuration and factory installed memory in the Master Stations only. In keeping with the desire to maximize integration, the use of any available contacts/connectivity on the door stations to unlatch the door at that station with the unlatch button on the intercom master station answering the call and/or to shunt an access control system “door force” alarm event is desirable.

34) Can you define what is a critical issue and what not? Can you provide examples?

A: A critical issue is defined as follows: Any system or hardware error covered by the maintenance agreement that prohibits a door from being physically secured 24/7/365, failure of any credentialing terminal, or complete system failure at any facility. All other issues are considered routine and may be handled next business day. Note that the Division maintains a separate maintenance agreement with a Datacard Group authorized service center for any physical hardware and firmware problems with the Datacard badge printers; as such printer service will not be included in the maintenance agreement.

Q: Can you please give the exact license count/coverage in the existing Open Options.

A: The Division owns 1 “client” license, 0 “badging” licenses, 1 “driver” license, and 10 “subcontroller” licenses. Both 1 client license and 1 subcontroller license are in use at Facility A; both doors on that subcontroller are included in the door/reader count total for this project.
35) Can you please give a firm door count for each building? The quote only gives readers, as there is a pricing difference between wiring up just a reader and an accountability reader.

A: Please see answer #13.

36) Can you please clarify the live view portion of cameras from the Orlando site to the ops center in Tallahassee?

A: Specific to the security cameras, facility C must have real-time video capabilities on the local equipment and network inside facility C, which is currently accomplished with the existing Panasonic DVR, monitor, and control stations. Given the extensive network needs for live video, the Division is comfortable with using the existing DVR web application to view these cameras across its network in Facilities A and B on an as-needed basis.

Specific to the intercoms, video from the intercoms should be viewable real-time during an intercom call only when the scheduling on door stations routes the call to master stations in Facility A.

37) Are other biometric options besides fingerprint a viable option?

A: No. Fingerprints are the standard to be used.

38) The Kiosk for visitor management, do you want a standalone kiosk or will it be mounted on the desk like the one you demonstrated?

A: Both options will be considered.

39) Can you please firm up mounting locations for head end equipment in each location?

A: In Facility A: there is space for 32 sq.ft. of wall board to be mounted. In Facility B: a minimum of 8-10 rack spaces are available in all communications closets as well as some wall board. In Facility C: 20+ rack spaces are available as well as approximately 6 sq. ft. of wall.

40) Are the open option door boards and intelligent controllers to be mounted in lockable cans or are they to be mounted in the existing racking systems?

A: See answer #39.

41) To meet the backup power requirements. Are we supposed to include the high voltage electrical work to hard wire the power supplies into the emergency power system or just an UPS capable of powering the units for 2 hours.

A: See answer #17.
42) In the service response time, to lessen the cost to the state would a 4 hour response time be more amenable as it is closer to what is normally done for critical emergency events.

A: We will consider both options and related pricing as clarified in question #20.

43) Is the Division now using Visitor scanning software of driver’s license cards that links to the Federal Sex Offender database? Or must the vendor provide this or other compatible software to bridge to the Fed database?

A: No. The current system does not link to the Federal Sex Offender Database. The functionality was provided as an example and may be quoted as an option; it is not a required element.

44) Will facility drawings with reader locations both existing and new doors be available to plan wire runs?

A: We have floor plans but do not have structural or electrical level drawings for the facilities. Locations of existing and new readers will be provided to vendor awarded the contract.

45) Will camera IP converters be acceptable for converting existing cameras in Facility A&B to IP to record to new Network recorder or must all analog cameras be replaced with IP cameras? If no, will a hybrid NVR be acceptable to record both analog and IP level cameras?

A: If the vendor is proposing strictly an IP based network video recorder (NVR), then converters will be acceptable and should be used unless it is more cost effective to replace all the existing analog cameras with IP cameras. A hybrid NVR is also acceptable, and the existing analog wiring terminates to the facility A “Watch Office” for all cameras in facilities A and B, and the network closet for all cameras in facility C.

If the vendor elects to specify a strictly IP based NVR and replacement cameras are needed, the exact camera count and type of existing cameras for facility A & B are below:

Facility A and B: 11 Bosch PTZ cameras (3 exterior pendant mount, 5 exterior wall bracket pendant mount, 3 interior ceiling mounted), 5 Bosch stationary cameras (all interior), and 4 analog looping outputs from a secondary analog DVR not controlled by our agency.

46) Facility C camera system: Must the existing Panasonic WJ-HD616 be replaced to comply with the 180 day video archive requirement?

A: No. The current system already records 180 days of data.
47) Will the Division prefer the same video management system for all facilities? This avoids confusion in the watch center.

A: We will consider all options with the intent of achieving the maximum level of integration against available funding. A single video management platform is highly desirable but replacement of the existing standalone DVR system and cameras at Facility C is one of the lowest priorities for available funding.