

**PALM BEACH COUNTY
BOARD OF COUNTY COMMISSIONERS
AGENDA ITEM SUMMARY**

Meeting Date: June 19, 2018

☒ Consent

☐ Regular

☐ Public Hearing

☐ Workshop

Department:

Submitted by: Information Systems Services (ISS)

Submitted for: Information Systems Services and Office of the Inspector General

I. EXECUTIVE BRIEF

Motion and Title: **Staff recommends motion to receive and file:** the Management Control Memorandum of Understanding ("MOU") between the Palm Beach Information Systems Services Department ("ISS") and the Palm Beach County Office of the Inspector General ("OIG") as required by the U.S. Department of Justice, Federal Bureau of Investigation Criminal Justice Information Services ("CJIS") Security Policy.

Summary: ISS provides various information technology services to the OIG, including data transport and network services used to operate OIG equipment and systems, voice services, systems design and programming, application hosting; and data backup and storage. Because the OIG is granted access to the National Crime Information Center (NCIC) and the Florida Crime Information Center (FCIC), the CJIS Security Policy requires that a formal Management Control MOU be entered into with any non-criminal justice agency, such as ISS. Countywide (DCB)

Background and Justification: The OIG offices are located in County-owned facilities that are connected to the County's network for data transport and internet access. ISS also provides other information technology services to the OIG, including application development and maintenance, application hosting, and data backup and storage. Any non-criminal justice agency, such as ISS, with access to criminal justice information is required to be a party to a Management Control agreement as stipulated in the CJIS Security Policy, Section 5.1.1.4:

"5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department."

Continued on page 3...

Attachments:

1. Management Control Memorandum of Understanding dated May 30, 2018

Recommended by:	<u>Steve Bordelon</u>	6-4-2018
	Department Head	Date
Approved by:	<u>[Signature]</u>	4/13/18
	County Administrator	Date

II. FISCAL IMPACT ANALYSIS

A. Five Year Summary of Fiscal Impact

Fiscal Years	<u>2018</u>	<u>2019</u>	<u>2020</u>	<u>2021</u>	<u>2022</u>
Capital					
Expenditures	(\$0)	(\$0)	(\$0)	(\$0)	(\$0)
Operating Costs	\$0	\$0	\$0	\$0	\$0
External Revenues	\$0	\$0	\$0	\$0	\$0
Program Inc (County)	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>
In-Kind Match (County)	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>
NET FISCAL IMPACT	<u>(\$0)</u>	<u>(\$0)</u>	<u>(\$0)</u>	<u>(\$0)</u>	<u>(\$0)</u>

Additional FTE

Positions (Cumulative)	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>
------------------------	----------	----------	----------	----------	----------

Is Item Included in Current Budget Yes X No

Does this item include use of federal funds? Yes _____ No X

Expenditure Budget Number: Fund Dept _ Unit Object

B. Recommended Sources of Funds / Summary of Fiscal Impact

C. Department Fiscal Review: K. F. Keen 6/6/18

III. REVIEW COMMENTS

A. OFMB Fiscal and/or Contract Development & Control Comments:

[Signature] 6/2/18
 [Signature] 6/14/18
 OFMB Contract Administration
 (47) (20) 6/4/18 6/4/18
 AK 6/7/18
 6/12/18

B. Legal Sufficiency:

 6/14/18
Assistant County Attorney

C: Other Department Review:

Department Director

THIS SUMMARY IS NOT TO BE USED AS A BASIS FOR PAYMENT.

Continued from page 1...

ISS service costs applicable to the OIG are determined based on the ISS annual cost allocation plan. The OIG's allocated costs are budgeted each year in their operating budget and ISS bills the OIG for one-twelfth (1/12) of these costs on a monthly basis for Enterprise Services and bills for Professional Services (programming) at the rate of \$85 per hour. A total of \$146,127 is budgeted for ISS service costs in the OIG's FY 2018 operating budget.

The Board has previously approved management control agreements for IT services provided to the Palm Beach Sheriff's Office and the Palm Beach County State Attorney's Office.

Management Control Memorandum of Understanding

This Management Control Memorandum of Understanding (MOU), dated as of this 30th day of MAY, 2018, is between the Palm Beach County Information Systems Services (ISS) and Palm Beach County Office of Inspector General (OIG) within Palm Beach County. This MOU sets forth their mutual understanding pertaining to technology services provided by ISS to the OIG to include: data transport and network services used to access OIG equipment and systems; voice services; systems design and programming; application hosting; data backup and storage; and operational procedures associated with the development, implementation, and maintenance of the OIG system, and access to the Florida Crime Information Center (FCIC) programs.

WITNESSETH

WHEREAS, the OIG is a criminal justice agency formally recognized by the Federal Bureau of Investigations (FBI) and the Florida Department of Law Enforcement (FDLE); and

WHEREAS, the OIG has been granted access to the Florida Criminal Justice network (CJNet), the National Crime Information Center (NCIC), the Florida Crime Information Center, and the Interstate Identification Index (III), all hereafter collectively referred to as FCIC, via network connectivity to the FDLE; and

WHEREAS, in exchange for access to the FCIC, the OIG has agreed to comply with the U.S. Department of Justice, FBI Criminal Justice Information Services (CJIS) Security Policy; and

WHEREAS, ISS serves as the primary information technology (IT) support agency for most of the departments reporting to the Palm Beach County Board of County Commissioners, the independently elected constitutional officers of Palm Beach County, and the OIG;

NOW THEREFORE, in consideration of the mutual covenants contained herein, and for good and valuable consideration, ISS and OIG agree as follows:

- (1) The Recitals to this MOU are incorporated herein by this reference with the same force and effect as if set forth in full.
- (2) ISS and OIG agree that OIG has authority to set, maintain, and direct ISS with respect to administration of that portion of the Palm Beach County computer systems and network infrastructure interfacing directly or indirectly with the FCIC. ISS and OIG agree that management control of the criminal justice function remains solely with the OIG and that nothing in this MOU recognizes or designates ISS as a criminal justice agency.

ISS shall provide the OIG within five (5) days of the execution of this MOU a list of all ISS personnel or contractors/subcontractors who will have physical and/or logical access to the network accessing, processing, storing, or transmitting Criminal Justice Information (CJI) from FCIC that is accessible to the OIG. Prior to authorizing those individuals to access the network or any component thereof accessing, processing, storing, or transmitting CJI from FCIC that is accessible to the OIG, ISS shall certify to the OIG that such personnel and contractors/subcontractors have satisfactorily completed a national Level II fingerprint-based background check under the OIG's Originating Agency Identifier Number (ORI) and Level 4 Security Awareness Training. Level 4 Security Awareness Training must be completed at least biannually. ISS shall have an ongoing obligation to ensure that background checks and training requirements are current and up-to-date. In the event that ISS receives notice that a person who has access to CJI is subsequently arrested and or convicted, ISS shall immediately upon receiving such notice, terminate the individual's access to the network or any component thereof accessing, processing, storing, or transmitting CJI from FCIC that is accessible to the OIG.

(3) If ISS terminates a member of the ISS support team, or terminates a contract with a contractor who has access, the OIG will be notified and all rights and privileges for that individual will be immediately revoked. ISS will update and maintain a current list of individuals who have access and provide the list to the OIG whenever a change occurs, but at a minimum, on an annual basis.

(4) ISS will ensure the OIG network is monitored at all times for any security related incidences or intrusions. If found, ISS will notify the OIG immediately and work to contain the breach and limit the loss of data or system integrity. If ISS outsources to a third party vendor to manage or maintain its IT system, ISS shall consult with the OIG for guidance regarding personnel and access prior to allowing the third party any physical or logical access to the criminal justice network.

(5) The OIG General Policy and Procedures for Criminal Justice Information Services Compliance Policy OIG-O-022 is attached hereto as Exhibit A. ISS agrees to comply with OIG-O-022 and CJIS Security Policy in regards to personnel and the maintenance and upkeep of the criminal justice network.

(6) This MOU shall be construed by and governed by the laws of the State of Florida.

(7) This MOU represents the entire understanding between the parties, and supersedes all prior negotiations, correspondence, understandings, representations, or agreements, either written or oral, relating to the issues set forth in this MOU.

PALM BEACH COUNTY INFORMATION SYSTEMS SERVICES

APPROVED AS TO FORM AND
LEGAL SUFFICIENCY:

By: Steve Bordelon
Steve Bordelon
Chief Information Officer, ISS

By: [Signature]
County Attorney

PALM BEACH COUNTY OFFICE OF INSPECTOR GENERAL

By: [Signature]
John Carey, Inspector General

To: Employees of the Office of Inspector General, Palm Beach County, Florida

From: Sheryl Steckler, Inspector General

Prepared by: Director of Investigations

Subject: CJNet Security Incident Response

PPM#: OIG-O-022

ISSUE DATE	EFFECTIVE DATE
February 14, 2013	February 14, 2013

PURPOSE:

The purpose of this policy is to outline the requirements identifying, reporting and resolving computer security incidents as they relate to CJNet and related systems.

BACKGROUND:

On August 28, 2012, the OIG (User) was approved as a Criminal Justice Agency by the FBI and the Florida Department of Law Enforcement (FDLE). As such, the OIG was provided with access to (CJNet) which is an intra-agency information and data sharing network for use by the State’s criminal justice agencies. Access to this system allows the OIG to query several databases which provide, among other information, criminal history records on individuals.

AUTHORITY:

Office of Inspector General, Palm Beach County
Florida Department of Law Enforcement
Federal Bureau of Investigation

POLICY OVERVIEW:

The Criminal Justice Information Services (CJIS) Security Policy and the CJIS Certification Training Manual provide specific guidance on the handling of security incidents. These documents are available for the OIG personnel who have assigned CJNet responsibilities.

The Criminal Justice User Agreement, entered into between the Inspector General and the FDLE, requires that the User “...must have a written policy documenting the actions to be taken in response to a possible computer security incident.”

RESPONSIBILITIES:

The designated Terminal Agency Coordinator or the Assistant Terminal Agency Coordinator will immediately report any suspected breach of the CJNet to the Local Agency Security Officer (LASO).

The LASO will be responsible for identifying, reporting, investigating and recovery from computer security incidents. The LASO will coordinate with FDLE on all CJNet security incidents.

The CJIS Certification Training Manual requires that the FDLE Information Security Officer (ISO) will be immediately notified of any suspected compromise of the CJNet. This notification will be made via email at: CJISCSO@fdle.state.fl.us and the message subject line should read "Possible Security Incident". The email should include the following information: date of the incident, location(s) of the incident, systems affected, method of detection, nature of the incident, description of the incident, actions taken/resolution and contact information for the agency (LASO).

Palm Beach County PPM CW-O-059, Information Resource Security Program Policies, Section 19.4, outlines the County's procedures to be followed in response to a computer security incident and the responsibilities of the Systems Administrator (LASO).

ALL information Technology (IT) personnel who must have access to the FCIC II message switch must also complete CJIS Online Security Training provided by FDLE.

The LASO will be responsible for logging the information relative to the suspected incident or breach including the following:

- Dates and times of incident related phone calls and meetings
- Individuals contacted
- Identification of systems, programs or networks that have been affected
- Dates and times when incident related events were discovered or occurred; amount of time spent working on incident related tasks.

CJIS Security Policy, Section 3.2.9, Local Agency Security Officer (LASO) requires that each LASO shall:

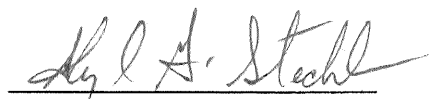
1. Identify who is using the CJIS Systems Agencies (CSA) approved hardware, software and firmware and ensure no unauthorized individuals or processes have access to same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

The LASO will also be responsible for notifying FDLE immediately, should an FCIC/NCIC workstation malfunction or become inoperable.

CONSEQUENCES OF POLICY VIOLATION

FDLE reserves the right to terminate service, without notice, upon presentation of reasonable and credible evidence that the User is violating the Agreement or any pertinent federal or state law, regulation or rule.

Any violation of this policy can result in the termination of the OIG's access to the CJNet.



Sheryl G. Steckler
Inspector General
Palm Beach County