HONORABLE JOHN D. BATES
Director

JILL C. SAYENGA
Deputy Director

ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS

WASHINGTON, D.C. 20544

LAURA C. MINOR
Associate Director

Department of Program Services

April 24, 2014

MEMORANDUM

To: Federal Public/Community Defenders

From: Laura C. Minor, Associate Director Laura C. Minor

RE: AOUSC REORGANIZATION AND THE MOVE OF DEFENDER SERVICE IT STAFF **(INFORMATION)**

In June, 2013, the Director announced his plans to restructure the Administrative Office. His goal was to reduce operating costs and duplication of effort, simplify the agency's administrative structure, and provide enhanced service to the courts and the Judicial Conference. In an effort to accomplish these objectives, a consolidation of information technology resources was implemented. This meant that Defender Services Office IT staff would no longer be supervised by Defender Services Office (DSO) but would be supervised by the Case Management Systems Office (CMSO).

This move caused concerns with the defender community that ethical responsibilities of client confidentiality could potentially be compromised. After listening to all of the concerns, I created a "tiger team" that included me, members of my immediate staff, DSO leadership, CMSO leadership (including members of Defender IT), the Office of General Counsel, and two Federal Public Defenders. We worked through the issues and drafted the attached memoranda of understanding (MOUs) to cover (1) control of and access to Defender applications, systems, and data; (2) the supervision and administration of NITOAD by CMSO and the Federal Public Defender's Office for the Western District of Texas (TXW); and (3) an agreement on how Defender IT support responds to information and system-related requests from entities external to the DSO.

In addition to the signatories of these documents, they have now been reviewed and approved by the Judicial Conference Committee on Defender Services, the Defender Services Advisory Group, and the Defender Services Automation Working Group. We believe that by following the procedures outlined in the MOUs, we can meet the goals of

the AO restructure while providing you and your staff members access to a greater number of information technology specialists to assist with development of defender centered applications. This additional group of resources, along with more standardized business processes, will improve the ability of DPS to deliver quality solutions to meet your client needs. By following the processes currently in place for managing data, which are modified by this agreement to conform to new organizational structure, we will be able to protect the confidentiality of your data.

Please know that protecting your sensitive client and representation-related data is of paramount concern to me and to the leadership of the AO, the DSO, and the CMSO. You and DSO are the owners of the data in defender applications. We will work with diligence to ensure we are successful in this important responsibility.

I want to thank you for all of your patience as we worked through this, and for your support in helping us meet the goals of the agency.

3 Attachments

Defender System Information Requests

Memorandum of Understanding

between

AO DPS Defender Services Office

and

AO DPS Case Management Systems Office

Final February 27, 2014

TABLE OF CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

The reorganization within the Administrative Office of the United States Courts (AOUSC) went into effect on October 1, 2013. Under the new structure, the former Office of Defender Services Information Technology Division (ODS ITD), including the National IT Operations and Applications Development, is moved from the Defender Services Office (DSO, formerly called the Office of Defender Services (ODS)) to the Case Management Systems Office (CMSO) and renamed Defender IT Support. The Defender IT Support staff and NITOAD Branch will continue to manage and maintain the Defender Services Program's applications and systems while part of the CMSO. DSO will maintain a Defender IT Liaison position to act as liaison between CMSO and DSO. The NITOAD Branch will remain employees of the Federal Public Defender for the Western District of Texas (FPD-TXW), will be funded through the Defender Services account, and will function under the operational control of the Defender IT Support Chief.

1.2 PURPOSE AND OBJECTIVES

This Agreement outlines the terms and conditions under which Defender IT Support responds to information and system-related requests from entities external to the DSO. Its objective is to provide a framework to deliver timely and quality reports and services while preventing inadvertent release of sensitive data or information which could violate Defender clients' attorney-client privilege, Defender work product privilege, or the ethical responsibilities of FDO staff or CJA panel attorneys using these applications.

1.3 PARTIES TO THE AGREEMENT

This Agreement is made between:

- the Chief, CMSO, and
- the Chief, DSO, and
- the Associate Director, supervisory department for CMSO and DSO, the Department of Program Services (DPS) of the Administrative Office of the United States Courts, located within the Thurgood Marshall Judiciary Building at One Columbus Circle, NE, Washington DC 20544**.**

1.4 COMMENCEMENT DATE

This Agreement begins the date all signatories give approval to enter into this Memorandum of Understanding – Defender Systems Information Requests.

1.5 AGREEMENT'S DURATION

This Agreement is valid from the date the DPS Associate Director signs this Agreement and is valid until otherwise superseded in writing and agreed to by all parties to this Agreement. Any signatory to this Agreement may terminate the Agreement effective 120 days from providing written intent of such to the other signatories or by future AO reorganization affecting any signatory department, division, office, or branch. In such event, the principal parties to this MOU will meet to resolve the issue prompting the proposed termination.

2 PERIODIC REVIEW

.
This Agreement should be reviewed a minimum of once a year. Failure to review once a year will not impede or cancel this Agreement.

The Defender IT Liaison and the Chiefs of Defender IT Support are responsible for facilitating regular reviews of this Agreement with the Chiefs of DSO and CMSO. This Agreement's content may be amended or modified as required provided all signatories mutually agree.

This Agreement will be posted to the Defender intranet website (DWeb) and DSO and CMSO network share drives to ensure it can be accessed by all stakeholders.

3 DEFINITIONS

ITEM	DEFINITION
CMSO	The Case Management Systems Office within the AO Department of Program Services.
CMSO Defender IT Support	Case Management Systems Office Defender IT Support staff, before re-organization working in the IT Division of the Office of Defender Services. This includes the NITOAD Branch.
defenderData	A COTS case management system, developed by JusticeWorks, which replaced the former in-house Defender Case Management System (CMS). This system contains federal defender representation, time use and other litigation sensitive and client confidential information/work product for use by the FDO and its defense teams, and from which workload and time data are reported to the AO. Unauthorized access to or disclosure of this litigation sensitive information would violate the attorney-client and work product privileges and the ethical responsibilities of Defender attorneys.
DSMIS	The Defender Services Management Information System, a data mart containing FDO- and CJA-related workload, financial, staffing, personnel, time use, and other relevant information, is accessed and used to support DSO oversight of the Federal Defender Program, to respond to internal and external inquiries, and by FDOs to monitor their local operations. This application is operated and maintained for DSO by Defender IT Support staff.
DSMIS Protocol	Rules published in the AO Manual, Volume 9, Chapter 1, § 140 Disclosure of Information from the Defender Services Management Information System (DSMIS) outlining the procedures and processes for release of information from DSMIS.
DSO	The Defender Services Office within the AO Department of Program Services.
DSO Chief Information Officer (CIO)	Primary person overseeing transfer of Defender information to external entities, the DSO Chief.
DSO CIO Designee	Person delegated temporary authority by the DSO CIO to oversee CIO responsibilities.
DSO Defender IT Liaison	Person within DSO acting as IT Liaison between CMSO and DSO.
DSO Systems Supported by Defender IT	A listing describing the various systems supporting the DSO and Defender Program, originally managed by the ODS IT Division and NITOAD Branch, which now fall under the purview of the CMSO. *November 27, 2013, Memo to Cait Clarke from George Drakulich*, outlining the defender systems supported by CMSO Defender IT Support.

External entity	Entities outside of the AO but within the Judicial Branch.
FDOs	Federal Defender Organizations. This term includes all Federal Public Defender Organizations (FPDOs) and Community Defender Organizations (CDOs).
Internal entity	Entities within the AO but outside of DSO
Lotus Notes	The email system used by the Judiciary (Courts, AO and Defenders) to exchange information. The Defender Lotus Notes Domain is supported and managed by NITOAD Branch for the Federal Defender Organizations (FDOs). The application is located on the Defender Wide Area Network (DWAN).
NITOAD Branch	The National IT Operations and Applications Development (NITOAD) Branch. Those employees of the Federal Public Defender for the Western District of Texas (FPD-TXW) who provide operational support, maintenance and helpdesk support for the various applications supporting the FDOs. While under the administrative control of the FPD-TXW, they are within Defender IT Support's operational control for the national role and funding of the systems they provide to the FDOs. However, the staff of the NITOAD Branch will remain as employees of, and under the administrative control of the FPD-TXW.
Non-judiciary entity	Entities outside of the Judicial Branch.
Data Owner	The Defenders own the data in the *defenderData* application. DSO owns DSMIS data, much of which is reported to the AO by the FDOs. DSMIS and *defenderData* applications (and others) are managed and maintained by Defender IT Support staff, including the NITOAD Branch. As owners of the data, the Federal Defenders and DSO are ultimately responsible for data release from and data transfers in these systems.
Change Control Board	Group constituted to review recommendations from the user community to make changes to the applications. Includes, but is not limited to changing the application by adding new capability, adjusting the format of screens, providing new reports, etc, which will enhance the application to the user. This group will determine the impact, cost and viability of the requested changes and work with the vendor to implement approved changes. The CCB does not have access to the data of individual FDOs.

4 SERVICES DESCRIPTIONS

The Defender IT Support is responsible for providing the following services for DSMIS and *defenderData*:

- Operations and maintenance (O&M);
- Enhancements, defect remediation;
- Training FDO personnel;
- Developing informational requests and reports.

4.1 OPERATIONS AND MAINTENANCE

To view the operations and maintenance procedures for DSMIS and *defenderData* systems, please refer to the corresponding contract/vendor task order.

4.2 ENHANCEMENTS AND DEFECT REMEDIATION

The process for enhancements and defect remediation to the DSMIS and *defenderData* applications are in the corresponding vendor task order with CMSO. The CMSO Defender IT Support staff and NITOAD Branch will establish and maintain appropriate modification and change control processes for each supported application/system through a Change Control Board (CCB) or other mechanism as appropriate. The membership for these processes may come from CMSO Defender IT Support, NITOAD Branch, DSO, or FDO stakeholders, as appropriate. These processes do not provide access to the individual FDO data within the applications.

4.3 TRAINING

The training provisions for the DSMIS and *defenderData* systems are in the corresponding vendor's task order.

4.4 SYSTEM MANAGEMENT, INFORMATION AND DATA REQUESTS

Release of some information either in DSMIS or *defenderData* may be controlled by the *Guide to Judiciary Policy*, Vol.20, § 820 *et seq* (Testimony and Production of Records) and/or Volume 7, Defender Services, Chapter 5, Disclosure of Information on CJA-Related Activities. If there is any question on whether or how to respond to a subpoena or request for records, information or testimony, the AO's Office of General Counsel should be contacted.

DSO and Defender IT Support staffs are responsible for ensuring quality service while addressing information requests as well as protecting defender information and data contained in the supported systems. As owner of DSMIS data, DSO must first approve the information request before routing it to Defender IT Support staff to compile for release, which shall be reviewed by DSO before release. As owner of *defenderData* data, the Defender whose Office's data has been requested must first approve the information request before routing it to Defender IT Support staff to compile for release, which shall be reviewed by the affected Defender before release. In the event a request bypasses DSO or the affected Defender and is submitted directly to Defender IT Support or CMSO, Defender IT Support is responsible for routing the request to the DSO CIO or designee or the affected Defender for review and approval before taking further action. The DSO and Defender IT Support staff responsibilities are:

Defender IT Support Responsibilities

- Ensure DSMIS access is not provided to anyone outside the DSO except those Defender IT Support staff required to use DSMIS in performing their duties and specifically designated FDO staff. While DSMIS is intended to provide Defender Services Program oversight information and support, and to respond to inquiries from internal and external entities, it was developed and is intended for DSO and Defender access only.
- Operate and manage DSMIS and *defenderData* to ensure the information required by the DSO staff and FDOs is available in a timely fashion.
- Work with the DSO staff to modify the DSMIS application to maintain its viability and responsiveness to its user's needs.
- Ensure appropriate protocols are observed and followed.
- Log incoming system-related information requests:
  - if sent to CMSO directly, send the request to DSO for processing and advise requester of the need to go through DSO first;
  - receive DSO (approved) request form with details prior to developing response;
  - design and develop operational reports and forward final product to DSO CIO or designee; and
  - track requests and ensure closure.
- Develop and maintain modification and change control protocols through Change Control Boards (CCBs) foe DSMIS and *defenderData*. The CCB's membership will include staff from both CMSO, DSO and others as appropriate to:
  - Manage application enhancements and/or
  - Remediate bugs/defects.
- Train FDO staff on the supported applications.

DSO Responsibilities

- Work with Defender IT Support to create a Standard Request Form (Name, Requester Affiliation, Date, Description, Priority, etc.). Proposed Draft attached.
- Ensure appropriate protocols are observed and followed. Receive incoming information requests/inquiries.
- DSO CIO or designee will determine whether the requests or inquiries should be addressed.
- DSO CIO or designee will determine the priority of approved requests.
- Obtain Information Request Form signoff by DSO Chief Information Officer or designee and forward it to the CMSO Defender IT Support or an internal DSO staff for processing
- Upon receipt of the processed request:
  - the DSO CIO or designee will ensure that the information has addressed request(s) accordingly
  - determine the level of coordination, if any, that is required with FDO(s) or Court(s) and provide a copy of the report or other documentation to the FDO(s) or Court(s)
  - upon assurance that all appropriate coordination and consultation has been accomplished, approve or deny release of report(s) or information to the requester
  - communicate final decision to Defender IT Support staff

5 POINTS OF CONTACT

The following are responsible for the deployment and ongoing support of this agreement:

Contact Person	Title / Role	Contact Information
Cait Clarke	Chief, DSO	202-502-3030
Andrew Zaso	Chief, CMSO	202-502-1319
John Fay	Supervisory Management Analyst CMSO Defender IT Support	202-502-1640

6 SUPPORTING DOCUMENTATION

The following referenced documentation contains the types of services and other relevant information available for Defender applications supported by the CMSO.

Documentation	Description
DSMIS Contract (USCA12F0426 /0001)	DSMIS task order with contractor Galindo Consulting Inc.
***defenderData* Contract (USCA11D0741)**	*defenderData* task order with contractor Justice Works
DSO Systems Supported by Defender IT	A listing describing the various systems supporting the Defender Services Program, originally managed by the ODS IT Division and the NITOAD Branch, Now moved to CMSO, (November 27, 2013*, Memo to Cait Clarke from George Drakulich*, outlining the defender systems supported by Defender IT Support).

7 AGREEMENT APPROVAL

DSO Chief — Date: 4/8/2014

CMSO Chief — Date: 4/8/14

DPS Associate Director — Date: 4/11/14

Defender Application Support and Access

Memorandum of Understanding

between

AO DPS Case Management Systems Office

and

CMSO Defender IT Support

and

National IT Operations and Applications Development Branch

and

AO DPS Defender Services Office

Final February 27, 2014

TABLE OF CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

The reorganization within the Administrative Office of the United States Courts (AOUSC) went into effect on October 1, 2013. Under the new structure, the former Office of Defender Services Information Technology Division (ODS ITD), including the National IT Operations and Applications Development (NITOAD) Branch (Federal Public Defender for the Western District of Texas (TXW) employees who provide the operational, maintenance and help desk support for various applications and systems supporting Federal Defender Organizations (FDOs)), is moved from the Defender Services Office (DSO, formerly called the Office of Defender Services) to the Case Management Systems Office (CMSO) and renamed Defender IT Support. The Defender IT Support staff and NITOAD Branch will continue to manage and maintain the Defender Services Program's applications and systems while part of the CMSO. DSO will maintain a Defender Liaison position to act as Liaison between CMSO and DSO. The NITOAD Branch will remain employees of the Federal Public Defender for the Western District of Texas, will be funded through the Defender Services account, and will function under the operational control of the Chief, CMSO Defender IT Support.

1.2 PURPOSE AND OBJECTIVES

This Agreement outlines the terms and conditions under which the CMSO Defender IT Support and the NITOAD Branch will operate, function and control access to Defender applications and systems they support. Its objectives are to provide a framework for controlled and limited access to Defender applications and systems and the data and information they contain, to prevent inadvertent release of sensitive data or information which could violate Defender clients' attorney-client privilege, Defender work product privilege, or the ethical responsibilities of FDO staff or CJA panel attorneys using these applications.

1.3 PARTIES TO THE AGREEMENT

This Agreement is made between:

- the Federal Defender for TXW,
- the Chief, NITOAD Branch, located at the Northwest Center, IH 10, San Antonio, Texas,
- the Chief, CMSO Defender IT Support,
- the Chief, CMSO,
- the Chief, DSO, and
- the Associate Director, supervisory department for CMSO and DSO, the Department of Program Services (DPS) of the Administrative Office of the United States Courts, located within the Thurgood Marshall Judiciary Building at One Columbus Circle, NE, Washington DC 20544**.**

1.4 COMMENCEMENT DATE

This Agreement begins the date all signatories give approval to enter into this Memorandum of Understanding – Defender Application Support and Access.

1.5 AGREEMENT'S DURATION

This Agreement is valid from the date the DPS Associate Director signs this Agreement and is valid until otherwise superseded in writing and agreed to by all parties to this Agreement. Any signatory to this Agreement may terminate the Agreement effective 120 days from written intent of such to the other signatories or by future AO reorganization affecting any signatory department, division, office, or branch. In such event, the principal parties to this MOU will meet to resolve the issue prompting the proposed termination.

2 PERIODIC REVIEW

.
This Agreement should be reviewed a minimum of once a year. Failure to review once a year will not impede or cancel this Agreement.

The CSMO Defender Liaison and the Chiefs of CMSO Defender IT Support and NITOAD are responsible for facilitating regular reviews of this Agreement with the Chiefs of DSO and CMSO. This Agreement's content may be amended or modified as required provided all signatories mutually agree.

This Agreement will be posted to the Defender intranet web site (DWeb) and DSO and CMSO network share drives to ensure it can be accessed by all stakeholders.

3 DEFINITIONS

ITEM	DEFINITION
CMSO	The Case Management Systems Office within the AO Department of Program Services.
CMSO Defender IT Support	Case Management Systems Office Defender IT Support staff, reports to the Chief, CMSO. This function, before re-organization was the IT Division of the Office of Defender Services. This entity includes the NITOAD Branch as a subordinate element.
defenderData	A COTS case management system, developed by JusticeWorks, which replaced the former in house Defender Case Management System (CMS). This system contains federal defender representation, time use and other litigation sensitive and client confidential information/work product for use by the FDO defense team and from which workload and time data are reported to the AO. Unauthorized access to or disclosure of this litigation sensitive information would violate the attorney-client and work product privileges and the ethical responsibilities of the attorneys.
DSMIS	The Defender Services Management Information System, a data mart containing FDO- and CJA-related workload, financial, staffing, personnel, time use, and other relevant information, is accessed and used to support DSO oversight of the Federal Defender Program, to respond to internal and external inquiries, and by FDOs to monitor their local operations. This application is now operated and maintained for DSO by CMSO Defender IT Support staff.
DSMIS Protocol	Rules published in the AO Manual, Volume 9, Chapter 1, § 140 Disclosure of Information from the Defender Services Management Information System (DSMIS) outlining the procedures and processes for release of information from DSMIS.
DSO	The Defender Services Office within the AO Department of Program Services.
DSO Chief Information Officer (CIO)	Primary person overseeing transfer of Defender information to external entities, the DSO Chief.
DSO CIO Designee	Person delegated temporary authority by the DSO CIO to oversee CIO responsibilities.
DSO Defender Liaison	Person within DSO acting as Liaison between CMSO and DSO.
DSO Systems Supported by Defender IT	A listing describing the various systems supporting the DSO and Defender Program, originally managed by the ODS IT Division and NITOAD Branch, which now fall under the purview of the CMSO. *November 27, 2013, Memo to Cait Clarke from George Drakulich*, outlining the defender systems supported by CMSO Defender IT Support.

External entity	Entities outside of the AO but within the Judicial Branch.
FDOs	Federal Defender Organizations. This term includes all Federal Public Defender Organizations (FPDOs) and Community Defender Organizations (CDOs).
Internal entity	Entities within the AO but outside of DSO
Lotus Notes	The email system used by the Judiciary (Courts, AO and Defenders) to exchange information. The Defender Lotus Notes Domain is supported and managed by NITOAD Branch for the Federal Defender Organizations (FDOs). The application is located on the Defender Wide Area Network (DWAN).
NITOAD Branch	The National IT Operations and Applications Development (NITOAD) Branch. Those employees of the Federal Public Defender for the Western District of Texas (TXW) who provide operational support, maintenance and helpdesk support for the various applications supporting the FDOs. While under the administrative control of the TXW FPDO, they are within CMSO Defender IT Support's operational control for the national role and funding of the systems they provide to the FDOs. However, the staff of the NITOAD Branch will remain as employees of, and under the administrative control of the TXW FPDO.
Non-judiciary entity	Entities outside of the Judicial Branch.
Data Owner	The Defenders own the data in the *defenderData* application. DSO owns DSMIS data, much of which is reported to the AO by the FDOs. DSMIS and *defenderData* applications (and others) are managed and maintained by CMSO Defender IT Support staff, including NITOAD Branch. As owners of the data, the Federal Defenders and DSO are ultimately responsible for data release and data transfers regarding these systems.
Change Control Board	Group constituted to review recommendations from the user community to make changes to the applications. Includes, but is not limited to changing the application by adding new capability, adjusting the format of screens, providing new reports, etc, which will enhance the application to the user. This group will determine the impact, cost and viability of the requested changes and work with the vendor to implement approved changes. The CCB does not have access to the data of individual FDOs.

4 SERVICES DESCRIPTIONS

The CMSO Defender IT Support and NITOAD Branch are responsible for providing the following services for a variety of IT applications supporting the FDOs:

- Operations and maintenance (O&M);
- Enhancements, defect remediation;
- Training FDO personnel;
- Developing operational reports for management reviews;
- Coordinating with other organizations which may provide hardware and software support to ensure the efficient operation of these applications;
- Identifying the O&M costs associated with these applications for inclusion in the Defender Services budget.

4.1 OPERATIONS AND MAINTENANCE

To view the operations and maintenance procedures for DSMIS and *defenderData* systems, please refer to the corresponding contract/vendor task order. In addition, the NITOAD Branch staff operates and maintains the FDO's Lotus Notes domain.

4.2 ENHANCEMENTS AND DEFECT REMEDIATION

The process for enhancements and defect remediation to the DSMIS and *defenderData* applications are in the corresponding vendor task order with CMSO. The CMSO Defender IT Support staff and NITOAD Branch will establish and maintain appropriate modification and change control processes for each supported application/system through a Change Control Board (CCB) or other mechanism as appropriate. The membership for these processes may come from CMSO Defender IT Support, NITOAD Branch, DSO, or FDO stakeholders, as appropriate. These processes do not provide access to the individual FDO data within the applications.

4.3 TRAINING

The training provisions for the DSMIS and *defenderData* systems are in the corresponding vendor's task order.

4.4 SYSTEM MANAGEMENT, INFORMATION AND DATA REQUESTS

DSO staff, CMSO Defender IT Support staffs, and the NITOAD Branch are responsible for ensuring quality service while protecting defender information and data contained in the supported systems. As providers of the national Defender Services Program's systems and applications, each must work with the CMSO to establish rules and procedures which will prevent the inadvertent release of sensitive data or information which could violate Defender clients' attorney-client privilege, Defender work product privilege, or the ethical responsibilities of FDO staff or CJA panel attorneys using these applications, and to provide a framework for controlled and limited access to the Defender applications and the data and information contained in those systems. The key responsibilities of each unit are:

CMSO Defender IT Support Responsibilities

- Ensure DSMIS access is not provided to anyone outside the DSO except those CMSO Defender IT Support staff required to use DSMIS in performing their duties and specifically designated FDO staff. While DSMIS is intended to provide

Defender Services Program oversight information and support, and to respond to inquiries from internal and external entities, it was developed and is intended for DSO and Defender access only.

- Operate and manage DSMIS and *defenderData* to ensure the information required by the DSO staff and FDOs is available in a timely fashion.
- Work with the DSO staff to modify the DSMIS application to maintain its viability and responsiveness to its user's needs.
- Develop and maintain modification and change control protocols through Change Control Boards (CCBs) or other control mechanisms established for each assigned application. Membership for these processes may come from CMSO Defender IT Support, NITOAD Branch, DSO, or FDO stakeholders, as appropriate.
- Ensure FDOs are notified regarding system changes, adjustments, or services associated with assigned Defender IT applications.
- Develop and submit to the appropriate DSO staff CMSO Defender IT Support budget requests for funding necessary to maintain and support DSMIS, *defenderData,* and other assigned applications for inclusion in the Defender Services account budget, with an information copy to the CMSO Chief.
- In conjunction with DSO and the NITOAD Branch, take appropriate action to remedy and advise Defenders of any breach, inadvertent access to or unauthorized access or release of information from the supported systems.
- All CMSO Defender IT Support staff must be alert and notify the CMSO Defender IT Support Chief, NITOAD Branch Chief, and the DSO Defender Liaison if any learn of any attempt to access, obtain, or disclose the data from any Defender IT application without appropriate approval.

DSO Responsibilities

- Work with CMSO Defender IT Support and NITOAD Branch to ensure that this MOU's intent to safeguard and protect the sensitive data and information contained in Defender IT applications/systems supporting the FDOs is achieved.
- Be alert and notify the DSO Chief, DSO Defender Liaison, the CMSO Defender IT Support Chief, and the NITOAD Branch Chief, if they learn of any attempt to access, obtain or disclose the data from any Defender IT application/system without appropriate approval.
- Ensure FDOs are notified regarding system changes, adjustments, or services associated with the Defender IT systems.
- Ensure the agreements and protocols established for protecting and securing Defender applications are observed and followed.
- In conjunction with the CMSO Defender IT Support and NITOAD Branch, take appropriate action to remedy and advise Defenders of any breach, inadvertent access to or release of information from the supported systems.
- Participate in reviewing and approving application/system enhancements when appointed to appropriate Change Control Boards (CCBs) or other control mechanisms.
- Ensure requests for funding to continued effective operation and support to Defender IT applications and systems are included in the Defender Services account budget.

NITOAD Branch Responsibilities

- Ensure that access to supported Defender applications/systems is not provided to anyone except those FDO employees specifically identified by the local Defender to have access to the office's information.
- Specific, limited application access will be allowed for NITOAD Branch staff involved in the management and/or operating of an application/system (i.e., the two NITOAD Branch Lotus Notes Domain Administrators, the NITOAD Branch manager of the Defender Video Conferencing System)
- In addition, specific, limited application (not data) access will be allowed for CMSO Defender IT Support and DSO staff engaged in managing and/or operating an application/system (i.e., CMSO Defender IT Support Program Manager for *defenderData*).
- Ensure appropriate procedures are in place and observed to assure the Federal Defender community that their data is secure and not open or available to unauthorized individuals or entities.
- Work with DSO and CMSO Defender IT Support staffs to ensure this MOU's intent to safeguard and protect the sensitive data and information contained in Defender IT applications/systems supporting the FDOs is achieved.
- Provide appropriate levels of security and control over these applications to maintain the required restricted access.
- Participate in managing and/or maintaining Defender Services applications/systems and the Defender Wide Area Network (DWAN) as appropriate.
- Participate in and/or manage application/system enhancements through appropriate Change Control Boards (CCBs) or other control mechanisms.
- Be alert and notify the NITOAD Branch Chief, Defender IT Support Chief, and the DSO Defender Liaison if any learn of any attempt to access, obtain or disclose the data from any Defender IT application without appropriate approval.
- Provide FDO training on the applications identified.
- Ensure FDO notification regarding system changes, adjustments, or services associated with the Defender IT applications/systems.
- In conjunction with the CMSO Defender IT Support and DSO, take appropriate action to remedy and advise Defenders of any breach, inadvertent access to or release of information from the supported systems.
- Develop and submit their budget funding requests, necessary to support and maintain Federal Defender IT systems and applications, to the appropriate DSO staff for inclusion in the Defender Services account budget, with an information copy to the CMSO Defender IT Support Chief.

5 POINTS OF CONTACT

The following are responsible for the deployment and ongoing support of this agreement:

Contact Person	Title / Role	Contact Information
Cait Clarke	Chief, DSO	202-502-3030
Andrew Zaso	Chief, CMSO	202-502-1319
Maureen Franco	Federal Public Defender, Western District of Texas	915-534-6525
John Fay	Supervisory Management Analyst CMSO Defender IT Support	202-502-1640
Rafael Delgado	Chief, NITOAD Branch	210-308-3210

6 SUPPORTING DOCUMENTATION

The following referenced documentation contains the types of services and other relevant information available for Defender applications supported by the CMSO.

Documentation	Description
DSMIS Contract (USCA12F0426 /0001)	DSMIS task order with contractor Galindo Consulting Inc.
***defenderData* Contract (USCA11D0741)**	*defenderData* task order with contractor Justice Works
DSO Systems Supported by Defender IT	A listing describing the various systems supporting the Defender Services Program, originally managed by the ODS IT Division and the NITOAD Branch, Now moved to CMSO, (November 27, 2013*, Memo to Cait Clarke from George Drakulich*, outlining the defender systems supported by Defender IT Support).

7 AGREEMENT APPROVAL

Federal Defender, Western District of Texas — Date: 4/3/14

NITOAD Branch Chief — Date: 4/4/2014

CMSO Chief — Date: 4/11/14

DSO Chief — Date: 4/8/2014

CMSO Defender IT Support Chief — Date: 4/11/2014

DPS Associate Director — Date: 4/11/14

NITOAD Branch Operational and Administrative Supervision

Memorandum of Understanding

between

AO DPS Case Management Systems Office

and

Federal Public Defender for Texas Western

and

National IT Operations and Applications Development Branch

and

AO DPS Defender Services Office

Document Version:	Final
Date:	February 27, 2014

TABLE OF CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

The reorganization of the Administrative Office of the United States Courts (AOUSC) went into effect on October 1, 2013. Under the new structure, the former Office of Defender Services Information Technology Division (ODS ITD) was realigned to the new Case Management Systems Office (CMSO) as Defender IT Support. This revised structure for the Defender IT Support and the National IT Operations and Applications Development (NITOAD) Branch (Federal Public Defender for the Western District of Texas (TXW) employees who provide the operational, maintenance and help desk support for various applications and systems supporting Federal Defender Organizations). Ensuring the CMSO Defender IT Support and the NITOAD Branch can continue to manage and maintain the Defender Services Program applications and systems at or above the support levels previously provided is essential. The delineation of operational supervision, administrative management, business processes, and funding between the CMSO, DSO, Federal Public Defender for the Western District of Texas (FPDTXW), and NITOAD Branch, through this memorandum of understanding, will ensure the continued national IT support for the Federal Defender community.

1.2 PURPOSE AND OBJECTIVES

This agreement outlines the terms and conditions under which the CMSO will provide operational supervision over the NITOAD Branch, the Federal Public Defender for the Western District of Texas (FPDTXW) will provide administrative management, and the DSO will provide funding and project direction. The objective is to provide a basis and framework for defining the “day-to day” operational supervision of the NITOAD Branch, the coordination required for administrative management, and the NITOAD Branch’s participation in DSO budgetary development and procurement of IT hardware, software, and services.

1.3 PARTIES TO THE AGREEMENT

This agreement is made between the Federal Public Defender for the Western District of Texas, located at 727 East Cesar E. Chavez, San Antonio, Texas, and the parties organizationally assigned to the Department of Program Services (DPS) of the Administrative Office of the United States Courts: CMSO Defender IT Support; Chief, Case Management Systems Office; and Chief, Defender Services Office; located at the Thurgood Marshall Federal Judiciary Building, One Columbus Circle, NE, Washington, DC 20544**.**

1.4 COMMENCEMENT DATE

This Agreement will commence on the date approval is obtained from all signatories.

1.5 DURATION OF THE AGREEMENT

This Agreement is valid from the signature date of the DPS Associate Director and is valid until otherwise noted. This agreement may be terminated by any of the signatories by providing one hundred and twenty (120) day notice of such intent to the other signatories. In such event, the principal parties to this MOU will meet to resolve the issue prompting the proposed termination.

2 PERIODIC REVIEW

.

This Agreement should be reviewed at a minimum of once per year; however, in lieu of any review in any period, this Agreement shall remain in effect.

The DSO Defender Liaison, the Chief, NITOAD Branch, and the Chief, CMSO Defender IT Support, are responsible for facilitating regular reviews of this document with the Federal Public Defender for the Western District of Texas, the Chief, DSO and the Chief, CMSO. Content of this Agreement may be amended or modified as required provided mutual agreement is obtained from all signatories.

This Agreement will be posted to the Defender intranet web site (DWeb) and to the DSO and CMSO network share drives to ensure it is accessible to all stakeholders.

3 DEFINITIONS

External entity	DEFINITION
	Entities outside of the AO but within the Judicial Branch.
CMSO	The Case Management Systems Office of the AO, Department of Program Services
CMSO Defender IT Support	Case Management Systems Office Defender IT Support staff previously (pre- re-org) working in the IT Division of the Office of Defender Services. This includes the NITOAD Branch.
defenderData	A COTS case management system, developed by JusticeWorks, which replaced the former in house Defender Case Management System. This system contains federal defender representation, time use, and litigation sensitive information/work product for use by FDO defense teams and from which selected workload and time data are reported to the AO. Unauthorized access to or disclosure of this litigation sensitive information would violate the attorney-client privilege and ethical responsibilities of the attorney.
DSMIS	The Defender Services Management Information System. A data mart which contains FDO and CJA related workload, financial, staffing, personnel, time use, and other relevant information which is accessed and used to support the DSO in its oversight of the Federal Defender Program and respond to internal and external inquiries, and by FDOs to provide insight into their local operation. This application is now operated and maintained for DSO by the CMSO Defender IT Support staff.
DSMIS Protocol	Agreement published in the AO Manual, Volume 9, Chapter 1, § 140 Disclosure of Information from the Defender Services Management Information System (DSMIS) outlining the procedures and processes for release of information from DSMIS.
DSO	The Defender Services Office of the AO, Department of Program Services
DSO Defender Liaison	Person within DSO designated as Liaison between CMSO and DSO.
DSO Systems Supported by Defender IT	A listing describing the various systems supporting the Defender Services Program, originally managed by the ODS IT Division and the NITOAD Branch, which now fall under the purview of the CMSO (November 27, 2013, Memo to Cait Clarke from George Drakulich, outlining the defender systems supported by CMSO Defender IT),
DSO Chief Information Officer (CIO)	Primary person overseeing transfer of Defender information to external entities. This person is the Chief, DSO
DSO CIO Designee	Person delegated temporary authority by the DSO CIO to perform DSO CIO responsibilities.

FDOs	Federal Defender Organizations. This term includes all Federal Public Defender Organizations (FPDOs) and Community Defender Organizations (CDOs).
Internal entity	Entities within the AO but outside of DSO.
Lotus Notes	The email system used by the Judiciary (Courts, AO and Defenders) to exchange information. The Defender Lotus Notes Domain is supported and managed by the NITOAD Branch for the FDOs. The application is located on the Defender Wide Area Network (DWAN).
NITOAD Branch	The National IT Operations and Applications Development (NITOAD) Branch. Those employees of the Federal Public Defender for the Western District of Texas (TXW) who provide national operational, maintenance, and help desk support for the various IT applications and systems supporting the FDOs. Because of their national role and the Defender Services account funding of the systems and services they provide to the FDOs, the NITOAD Branch has been placed within and under the operational control of the CMSO Defender IT Support. However, the staff of the NITOAD Branch will remain as employees of, and under the administrative control of, the TXW FPDO.
Non-judiciary entity	Entities outside of the Judicial Branch
Data Owner	The Defenders own the data contained in *defenderData*. DSO owns the data in the DSMIS, much of which is reported to the AO by the FDOs. These systems and others are supported and maintained by CMSO Defender IT Support staff which includes the NITOAD Branch. As owners of the data, the Federal Defenders and the DSO are ultimately responsible for data release and data transfers regarding these systems.

4 MANAGEMENT DELINIATION OVER THE NITOAD BRANCH

The NITOAD Branch members are employees of the Federal Public Defender for the Western District of Texas, funded through the Defender Services account as a separate organizational unit, to provide national information technology support for the Federal Defender Organizations.

Working through the CMSO Defender IT Support, the NITOAD Branch is responsible for providing the following services for a variety of IT applications, systems and contracts supporting the Federal Defender Organizations (FDOs) and the DSO:

- Operations and maintenance (O&M)
- Enhancements and defect remediation
- Guidance and consultation of IT purchases
- Assistance with hiring of Federal Defender IT staff
- Training of Federal Defender Organization personnel
- IT policy development and guidance
- Strategic planning and execution
- Coordinating with other organizations which may provide hardware and software support to ensure the efficient operation of these applications
- Identifying the O&M costs associated with these applications/systems for inclusion in the Defender Services account budget submission
- Execution of procurement actions and contract management

4.1 CMSO DEFENDER IT SUPPORT OPERATIONAL SUPERVISION

The CMSO is responsible for providing the management oversight of the Defender IT Support as part of the AO's reorganization. Incorporated in this oversight will be the "day to day" operational supervision and support of the NITOAD Branch to ensure the information technology needs and services, required by the FDOs, are met in a timely manner and are coordinated and consistent with the Judiciary goals, projects, and policies developed by the AO's Department of Technology and the CMSO.

The Defender IT Support will provide the operational supervision through the Chief and Deputy Chief of the NITOAD Branch. To observe and maintain the delineation of supervisory duties, the Defender IT Support will meet with the FPDTXW yearly. CMSO through Defender IT Support will provide the following areas of supervision and leadership:

- Project planning, coordination, support, and guidance
- Application design and development, in coordination with NITOAD and defender organizations, including DSAG and DAWG
- Developing funding requirements for operations and maintenance
- Strategic planning
- Policy development and enforcement
- Procurement execution of DSO IT budget
- Oversight of DSO IT contracts
- Development of NITOAD Branch budget in coordination with DSO
- Providing travel approval and authorization
- Participating in employee hiring and discipline
- Yearly evaluation of the Chief of the NITOAD Branch to be submitted to the FPDTXW

- Participation in the interview and selection of candidates for the Chief and Deputy Chief of the NITOAD Branch
-

4.2 ADMINISTRATIVE MANAGEMENT

The FPDTXW will retain the administrative management, control, and support for the NITOAD Branch. To observe and maintain the delineation of supervisory duties and administrative management, the FPDTXW will meet with the Defender IT Support yearly. The administrative management of the NITOAD Branch will include:

- Employee hiring and discipline
- Budget development, oversight, and execution of the NITOAD Branch operational expenses
- Procurement assistance for NITOAD Branch requirements
- Administrative assistance with processing of personnel, time and attendance, travel, shipping, and procurement actions
- Participate in the interview and selection of candidates for the Chief and Deputy Chief of the NITOAD Branch.

4.3 TRAINING

To ensure the NITOAD Branch staff can support the FDOs with newer technology and application releases, it is imperative that the NITOAD budget contain sufficient funding to allow each staff member to attend two weeks of technology training. The FPDTXW, Defender IT Support, and the NITOAD Branch will develop the yearly training allotment required for submission to DSO. DSO and CMSO will ensure that adequate funding for NITOAD staff training needs is available through the Defender Services Program appropriation.

4.4 NITOAD BRANCH RESPONSIBLITES

The NITOAD Branch provides national applications and services to the FDOs and DSO. Safeguarding the FDO client sensitive data is paramount and essential for maintaining the confidentiality and attorney-client privilege responsibilities. Therefore, it is critical that the NITOAD Branch operate in a manner that provides the upmost security of the FDO data.

The NITOAD Branch responsibilities are:

- Ensure that access to supported Defender applications/systems is not provided to anyone except those individuals in the FDOs specifically identified by the local Defender to have access to their information. In addition, specific, limited access will be allowed for CMSO Defender IT Support, NITOAD Branch, and DSO staff engaged in the management and/or operation of an application/system (i.e., the two NITOAD Branch Lotus Notes Domain Administrators, the NITOAD Branch manager of the Defender Video Conferencing System or the CMSO Defender IT Support Program Manager for *defenderData (*access to the application's training database)).
- Ensure that appropriate procedures are in-place and observed to assure the Federal Defender community that their data is secure and not open or available to unauthorized individuals or entities.

- Work with DSO and CMSO Defender IT Support staffs to ensure that the intent of this MOU to safeguard and protect the sensitive data and information contained in Defender IT applications/systems supporting the FDOs is achieved.
- Provide the appropriate levels of security and control of these applications to maintain the restricted access that is required.
- Participate in the management and/or maintenance of Defender Service applications/systems and the Defender Wide Area Network (DWAN) as appropriate.
- Participate in and/or manage application/system enhancements through appropriate Change Control Boards or other control mechanisms.
- All NITOAD Branch staff must be alert and notify the Chief, NITOAD Branch, Chief, Defender IT Support, and the DSO Defender Liaison if they learn of any attempt to obtain or disclose the data from any Defender IT application without appropriate approval.
- Provide training to Federal Defender Organizations on the applications identified.
- Ensure notification of the FDOs regarding system changes, adjustments, or services associated with the Defender IT applications/systems.
- In conjunction with the CMSO Defender IT Support and DSO, take appropriate action to remedy and advise Defenders of any breach, inadvertent access to, or release of information from the supported systems.
- The NITOAD Branch will develop and submit their budget requests for funding necessary to support and maintain Federal Defender IT systems and applications to the appropriate DSO staff element for inclusion in the Defender Services account budget with an information copy to the Chief, CMSO Defender IT Support.

4.5 DSO RESPONSIBILITES

To maintain necessary national FDO IT support, adequate funding is required for the NITOAD Branch. Additionally, the DSO needs to communicate strategies, projects, and policy requirements to the NITOAD Branch, through the CMSO Defender IT Support. Therefore, coordination is required between DSO, CMSO Defender IT Support, and NITOAD Branch to ensure the highest level of IT support is afforded the FDOs.

To achieve these goals, the DSO responsibilities are:

- Work with CMSO Defender IT Support and the NITOAD Branch to ensure that the intent of this MOU to safeguard and protect the sensitive data and information contained in Defender IT applications/systems supporting the FDOs is achieved.
- Ensure that requests for funding for continued and effective operation and support of Defender IT applications and systems are included in the Defender Services account budget.
- Participation in the interview and selection of candidates for the Chief and Deputy Chief of the NITOAD Branch
- All DSO staff must be alert and notify the Chief, DSO, the DSO Defender Liaison, the Chief, CMSO Defender IT Support, and the Chief, NITOAD Branch, if they learn of any attempt to access, obtain, or disclose the data from any Defender IT application/system without appropriate approval.
- Ensure the notification to FDOs regarding system changes, adjustments, or services associated with the Defender IT systems.

- Ensure that the agreements and protocols established for the protection and security Defender applications are observed and followed.
- In conjunction with the CMSO and the NITOAD Branch, take appropriate action to remedy and advise Defenders of any breach or inadvertent access to or release of information from the supported systems.
- Participate in the review and approval of application/system enhancements when appointed to appropriate Change Control Boards or other control mechanisms.

5 POINTS OF CONTACT

The following are responsible for the deployment and ongoing support of this agreement:

Contact Person	Title / Role	Contact Information
Cait Clarke	Chief, DSO	202-502-3030
Andrew Zaso	Chief, CMSO	202-502-1319
John Fay	Supervisory Management Analyst, CMSO Defender IT Support	202-502-1640
Rafael Delgado	Chief, NITOAD Branch	210-308-3210
Maureen Franco	Federal Public Defender for Texas Western	915-534-6525 x254

6 SUPPORTING DOCUMENTATION

The following documentation contains the types of services and other relevant information available for Defender applications supported by the CMSO.

Documentation	Description
DSMIS Contract (USCA12F0426 /0001)	DSMIS task order with contractor Galindo Consulting Inc.
***defenderData* Contract (USCA11D0741)**	*defenderData* task order with contractor Justice Works
DSO Systems Supported by Defender IT	November 27, 2013, Memo to Cait Clarke from George Drakulich, outlining the defender systems supported by CMSO Defender IT Support

7 AGREEMENT APPROVAL

Federal Public Defender for TXW	4/3/14 Date
Chief, NITOAD Branch	4/4/2014 Date
Chief, CMSO Defender IT Support	4/11/2014 Date
Chief, CMSO	4/8/14 Date
Chief, DSO	4/8/2014 Date
Associate Director, DPS	4/11/14 Date