Judicial Conference of the United States
Committee to Review the Criminal Justice Act Program

WRITTEN COMMENTS OF

HEATHER E. WILLIAMS,

FEDERAL DEFENDER, EASTERN DISTRICT OF CALIFORNIA

SAN FRANCISCO HEARINGS, MARCH 2-3, 2016

WRITTEN COMMENTS OF HEATHER E. WILLIAMS,
FEDERAL DEFENDER, EASTERN DISTRICT OF CALIFORNIA

Table of Contents

~ ~ ~ ~ ~

I. WITNESS'S BACKGROUND

I am the Federal Defender for the Eastern District of California (FD-CAE). Before my appointment here, I was with the Federal Public Defender, District of Arizona's Office (Tucson Division) for 19 years, eventually becoming that Office's First Assistant Federal Public Defender (AFD).

WRITTEN COMMENTS OF HEATHER E. WILLIAMS,
FEDERAL DEFENDER, EASTERN DISTRICT OF CALIFORNIA

1. Work Measurement Study Steering Group:

Around the time of my appointment, the Administrative Office directed the Defender Offices to participate in a work measurement study (WMS), the results of which would determine Defender budgets and staffing for at least five years. Participation in the study required standardizing timekeeping entries and case openings, as well as training all staff who would need to submit time.

In December 2013, Administrative Office of the U.S. Courts (AO) Director John Bates appointed eleven other Defenders and me to the WMS's Steering Group who, after analyzing data collection, would eventually recommend a staffing formula to the Judicial Resource Committee (JRC). The data reporting, collection, analysis, and recommendation needed to be completed by April 2015. Defenders changed timekeeping codes and case workload factors; I was among the Defenders producing nationwide webinars training on the new information.

The results showed Federal Defender Office (FDO)[1] staffs after sequestration were severely reduced and offices, putting in substantiated overtime, almost entirely needed additional staff and budgets, not less. The WMS formula the Steering Group eventually recommended to and was approved by the JRC allowed FDOs to hire staff positions best fitting the unique practices in each district. The formula, as applied to my FD-CAE Office, allowed us to started hiring again towards the end of FY 2015.

2. IT Tiger Team: Committee to Create Memoranda of Understanding Regarding Defender Services IT Application Access and National IT Operations and Applications Development Branch (NITOAD)*:*

After the AO's reorganization taking Defender Services Office (DSO) from a directorate level position to within the Department of Program Services, DSO IT was taken from DSO supervision to within Program Services' Case Management Systems Office (CMSO). A major part of our national IT, known as NITOAD, controlled our email, storage, and defenderData (dData: the program used to open and close FDO

[1] Throughout this *Comment, "*FDO" is also meant to include Community Defender Offices (CDOs).

cases, reporting our timekeeping, and record case weighted openings which are vital to determining our staffing and budgets).

Instantly, concerns arose over conflicts with the Judiciary having access to information likely containing attorney-client and work product privileged information. I was also part of the IT Tiger Team, a committee to create Memoranda of Understanding (a) limiting supervision and control over NITOAD, and (b) access to FDO electronically stored and generated information.

***3. 9th Circuit Capital Case Committee*:**

Recently, I was also appointed to the Ninth Circuit Capital Case Committee.

Originally named the "Ninth Circuit Death Penalty Task Force" when formed in 1987, and renamed the "Capital Case Committee" in the 1990s, the Committee made recommendations concerning capital case costs. In early 1996, the AO reported the Ninth Circuit spent more than 65% of the nation's total CJA capital habeas allotment, while having 23% of the nation's capital habeas cases. That year, the Ninth Circuit created the CJA Oversight Committee to address other CJA Ninth Circuit expenditures.

In the Fall 2003, the CJA Oversight Committee and Capital Case Committee were merged into the current Capital Case Committee. This Committee reviews District Court-approved case budgets (in trial level multi-defendant "mega-cases," federal direct death cases, and capital habeas cases) for reasonableness and suggests policies and procedures to provide effective representation while maintaining a stewardship obligation to the taxpayers' money.

II. COMMENTS CONCERNING CJA (18 U.S.C. §3006A), DEFENDER SYSTEM, AND THE JUDICIARY

1. Defender Services Office (DSO) – Directorate level: Restoring DSO to a Director level Department

a. DSO, while having always been within the Judiciary, has a separate budgetary allocation – none of it can be taken by the AO or the courts for

their use. Until 2014, The Office of Defender Services (ODS) was, within the AO organization, a directorate level office. *See Attachment 1.*

DSO is presently a division of the newly created Department of Program Services. *See Attachment 2.* Also in Program Services are Judicial Services, Court Services, Probation/Pretrial Services, Judiciary Data & Analysis, and Case Management Systems Office (CMSO). Each of the other Program Services divisions supports the work and functioning of the AO and the courts.

DSO does not support the functioning of the AO or the courts. DSO is constitutionally mandated (6th Amendment) and supports solely the representation of those indigent individuals involved with criminal charges considered by our federal courts.

> NACDL *Federal Indigent Defense 2015: The Independence Imperative*, p.5 (end notes omitted)
>
> … Laura Minor, the associate director of the Department of Program Services (and thus Ms. Clarke's immediate supervisor), told the Task Force that judges are the "policymakers" and Ms. Minor's job — and that of her staff — is to "support" the judges in their work. Her work is driven by "providing service to the courts" and "implementing the policies of the Judicial Conference," which means her own view of the Sixth Amendment right to counsel, for example, is "irrelevant." Ms. Minor's statements are consistent with her job description, which emphasizes her role is to "clarify[] and explain[] to others the importance of the judiciary's programs and legislative needs . . . ."

b. DSO, being a part of Program Services, has had to get approval to hire from Program Services. DSO's budget, and therefore DSO's staffing, is separate from the remainder of Program Services – Program Services cannot transfer any vacant DSO positions to any other area of Program Services.

Cait Clarke, at a recent FDO conference, reported, when she asked Program Services for permission to fill three positions, two of which have

been vacant for months, and one newly created with Program Services' consent (*see #2 below*), she was given authorization to only fill one position. – I did not see any posting to fill her position.

c. DSO's and the FDOs' full and prompt cooperation and participation in the WMS demonstrate our groups' willingness and ability to independently function again as a separate directorate level position. While the Judicial Council's approval of the proposed formulas seemed to have increased FDO respect with the AO, this has not trickled to Program Services, which insists on micromanaging DSO operations.

2. Special Deputy of Analytics and Information Management:

a. The now-approved WMS formulas for FDO staffing and budgets rely primarily upon Case Weighted Openings (CWOs).

Defender cases are opened using a case management program called defenderData (dData). When cases are opened, the charged statute(s) are input and generate a case weight or the CWO. If there are multiple charges, the highest case weight becomes the CWO.

The case weights were recently revised by RAND (called RAND 2), who proposed the original case weights implemented for Defender Offices about 5 years ago. Case weights were determined by the average number of hours all Defender Offices spent on each particular case type.

> The Judiciary has no control over the number and nature of cases (and, therefore CWOs) in which court-appointed counsel must provide a defense. The caseload is driven entirely by the prosecutorial policies and practices of the U.S. Department of Justice and its 93 United States Attorneys.

Statement Of Honorable Julia S. Gibbons, Chair Committee On The Budget Of The Judicial Conference Of The United States Before The Subcommittee On Bankruptcy And The Courts Of The Committee On The Judiciary Of The United States Senate (July 23, 2013).

Recent changes in DOJ charging policies are reducing the numbers and types of cases filed in court. Also, changes in case law (*Johnson v. United States*, June 2015 US Supreme Court decision about a statutory residual clause defining "crime of violence"), Sentencing Guidelines (retroactive 2 level Guideline reductions for drugs quantities), and statutory penalties (proposed changes to mandatory minimum sentences in firearms cases with retroactive applications) affect CWOs.

b. Program Services includes the Judiciary Data and Analysis Office where "Statisticians and analysts now work in one division, enabling greater collaboration and faster response to inquiries and changing circumstances." *Judge John D. Bates Memo,* ORGANIZATION OF OFFICES IN THE AO DEPARTMENT OF PROGRAM SERVICES (4/21/2014).

   More than ever, numbers, data, statistics, and probabilities control FDO and CDO budgets and staffing; they are entirely dependent upon the ever-shifting case and case type filings. DSO needs this Special Deputy position to monitor in real time these changes, immediately interpret the data, and propose reaction plans. Jon Sands, Federal Public Defender, District of Arizona, and head of Defender Services Advisory Group (DSAG), proposed an *Action Plan* incorporating the DSO position of *Special Deputy of Analytics and Information Management. DSAG Chair Jon Sands' letter to Cait Clarke (8/21/2015), and Action Plan*. As explained by Mr. Sands, "The Letter and Action Plan expressed the goals and proposals unanimously adopted by DSAG and PMWG after the adoption of the Work Measurement Study by the Judicial Conference." *Id.* This guarantees proactive and informed management decisions, resulting in budgetary savings.

3. Move Defender IT Support completely within DSO:

a. When reorganized, Defender IT was placed within CMSO in an effort to conserve and pool resources.

However, Defender IT supports and manages dData, Defender Services Management Information System (DSMIS), DSO/FDO/CDO email, and each Defender Office's IT. All servers supporting these are behind highly protected firewalls and are closely monitored to protect the attorney-client and attorney work product privileged material contained in each.

Because of the privileged nature of these processes, Memoranda of Understanding (MOUs) were created to:

- limit CMSO access to these processes,
- create a DSO Liaison position within DSO "to act as Liaison between CMSO and DSO," and
- confirm that National IT Operations and Applications Development (NITOAD) Branch would remain Federal Public Defender employees within the Western District of Texas Office.

Laura Minor Memo, AOUSC REORGANIZATION AND THE MOVE OF DEFENDER SERVICE [sic] IT STAFF (4/24/2014), for MOUs concerning *Defender System Information Requests* and *Defender Application Support and Access.* Attachment 3.

Even with these MOUs, I understand a newly hired Chief of CMSO's Defender IT Support Division, after being told of the MOUs' terms, tried to hack into DSMIS, when access by CMSO was specifically prohibited.

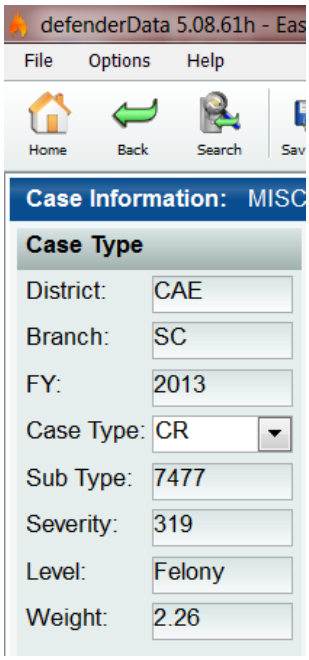
b. The reorganization has created unnecessary and multiple bureaucratic layers between DSO and the FDOs' needs and implementation.

Example: Making changes to dData to accommodate the case law/Guideline changes case types: NITOAD should have the ability to work directly with justiceworks (dData's creator) to make changes, which

can be done within days or weeks. However, if DSO wants to make a dData change, is must be worked through Defender IT Support Division (DITSD) Project Manager within CMSO. DITSD cannot access the actual data in dData because of privileges, so it must create a "sandbox" version to try to replicate the changes. There ends up being a delay in making changes and there may be secondary errors because the "sandbox" version may not have all affects dData components.

This would be avoided if NITOAD could control dData changes by having the Program Manager there.

c. *Example:* For years, I have worked to understand dData and its predecessor Case Management System (CMS), especially since, in 2011, the Defender system converted from case closings to CWOs to determine staffing and budget. For instance, I learned, in cases with multiple counts, what was reported to DSO was the case weight related to the charge with the highest severity code; a "severity code" was assigned by and shared with the judiciary to weight their cases and was based upon the maximum possible statutory sentence. The challenge this presented to FDOs was the charge with the highest severity code was not always the charge with the highest case weight, creating an inaccurate picture of office case demands.



The change to CWO staffing/budgeting projections created an ability to monitor each office as the year progressed and, when possible, adjust to maintain current staff or create an opportunity for more staff. This monitoring is possible with dData, the program designed by Justice Works for Defender

system use. The more information dData provides, and the accuracy of that information, create Office stability. But it depends upon dData.

Before and during the WMS, the case weights were being reviewed, updated, and revised. These revised case weights, along with removing severity codes as the reporting control, eventually became part of the statistical data included in the WMS's recommended and approved staffing formula. This formula was approved by the Steering Group by April 2015.

The above image reflects a case which, without severity code, has a reporting CWO of 4.82, not 2.26. I use this number to work with my Chief AFD and Branch Supervisor in deciding case assignments, to not overload any one AFD, to provided balanced weighted caseloads so cases can actually get closed. It is a lot of extra work to not have the revised CWO readily available.

I and other Defenders requested Defender IT within CMSO to change dData case CWO field to the revised case weights without severity discussed above. This would allow FDOs to better monitor yearly CWO projections, to better regulate keeping current staff or to plan should CWOs drop.

I understand from talking with someone at Justice Works they have been ready to create this field since receiving the revised case weights about a year ago; they already input the RAND 2 revised case weights database to generate one of the reports they offer through dData. But they cannot, by contract, create the field without Defender IT authorization. I also understand that, had that ability to authorize been with NITOAD, the field would have been updated a year ago.

CMSO's Defender IT has been unresponsive.

d. Change is needed sooner, not later. We expect another WMS in 3 to 5 years. We have to deal with our data immediately to be good stewards and responsible employers.

4. Autonomy by Defender Services Committee (DSC)/DSO over Budget, Staffing, Process, and Communication:

a. Ability to pass requests on to Congress directly, the same as FJC and Sentencing Commission do.

Defenders realize they may have ruffled feathers by going directly to Judiciary staff during sequestration. We did this because our organization felt its needs were either not being represented or were being misrepresented, accused of not engaging on cost-savings measures. We are unique – 60% of Defender budgets go to staffing/payroll, 10% to rent, 10% to client representation. There was no room to cut to save jobs during sequester. We have no $20 billion airplane we can stop building.

b. Greater autonomy over budget execution and staff hires.

DSO's challenges in getting required approval for its own staff are noted above. FDOs have proven their staffing and budget acumen through sequestration and their full participation in the WMS.

c. *Defender Operations Manual.*

Since I started with the Defender program in 1994, our how-to bible has been our *Operations Manual.* While the *Guide to Judiciary Policy* can give us some process instruction, many portions specifically are not applicable to FDOs. Defenders were told at their recent Portland Conference that we are no longer able to amend or update our *Operations Manual*, that any changes must crawl through the many bureaucratic layers of Department of Program Services approval.

WRITTEN COMMENTS OF HEATHER E. WILLIAMS,
FEDERAL DEFENDER, EASTERN DISTRICT OF CALIFORNIA

Already, Chapter 18 concerning our case management - opening and closing cases, and timekeeping codes – has not been updated in almost two years to reflect changes for the WMS. Other chapters advise on the changing attorney ethical obligations, audit processes, staffing and IT. Without our ability to continually update **our** Guide, understanding **our** unique role in our criminal justice process, without conflict by those with decision-making power over our clients, leaves us to stagnate.

5. Megacases and Budgets:

The Ninth Circuit's Capital Case Committee identified some common factors explaining some of the high 9th Circuit capital habeas costs, several of which reflect the high level of capital habeas representation present in the Ninth Circuit:

1. Postcard (one page) denials in California.
2. No evidentiary hearing in California state appellate proceedings.
3. California's legal culture.
4. Decentralized decision-making.
5. Inadequate information.
6. No cost controls by the client.
7. Higher rates paid in the Ninth Circuit
8. Use of large civil law firms.
9. Death Penalty Resource Centers.

The Judicial Conference of the United States, in September 1997, mandated each circuit's Judicial Council create a review process for any death penalty habeas corpus case in that circuit where the CJA attorney compensation exceeded $100,000.

Responding to all the above, Ninth Circuit innovations now provide better representation while controlling costs. Some have been implemented in other districts too.

1. 1995 Capital Habeas Corpus Unit (CHU) Pilot Project in Central District of California, followed shortly after in California's Eastern District (mu Office). Seventeen FDOs now house CHUs.

2. Death Penalty District Court Law Clerks -, providing specialized advice to District judges in capital case issues - another Ninth Circuit innovation now implemented nationwide.
3. Model Capital Case Management Plans and Orders.
4. *Capital Punishment Handbook,* *http://www.ca9.uscourts.gov/district/guides/capital_punishment_handbook.pdf*.
5. CJA Supervising Attorney Pilot Project.
6. Case Management/Budgeting Software -- Created by staff for CJA attorneys and the courts to help better manage capital habeas cases.
7. Maximum hourly rates for attorneys, investigators, experts – revisited regularly.
8. Capital Habeas Intranet website with links to budgeting information, sample orders, etc.
9. Case Budgeting Attorneys who not only advise trial and habeas counsel, but also judges in creating and approving budgets. Further they survey FDOs and make CJA budget recommendations with the goal of matching the same quality of representation FDOs provide their clients.

As for megacase budgets, opportunities to share paralegal, investigator, or expert services must be balanced with each counsel's obligation to effectively represent individual clients. Shared services fall to conflicts of interest between clients – those who cooperate, who plead guilty, who go to trial, whose defenses are duress, lack of knowledge, minimal role. Joint defense agreements are rare and sometimes ill-advised.

In my brief time on the Capital Case Committee, and in reviewing thus far only capital habeas proposed budgets, I have seen a high level of budget consciousness by habeas counsel, by magistrate and district judges reviewing these budgets, and by my fellow Committee members. All these review take a lot of time by each person involved – from creation to final review. One must question whether the money spent for the time each person takes in this review process actually ends up saving taxpayer money.

6. CJA Panel in the California Eastern District (CAE):

CAE CJA Representative Scott Cameron and CAE Magistrate Judge Carolyn Delaney have offered fine information on CJA Panel practice in

California's Eastern District. Let me offer information directly responding to several of the Committee's concerns.

Even before initial appearances, our Office tries to determine whether my Office has a conflict in representing those scheduled for appearance. We try to locate CJA counsel ahead of the initial appearance for case my Office cannot accept. In prehearing attorney-client meetings, we ask defendants if they plan to retain counsel. For those who do not, we take client financial information and advise the court regarding counsel appointment.

My Offices each have a CJA Panel Administrator who locates CJA counsel on a rotating basis. These Administrators also review vouchers for facial compliance; math is taken care of by eVoucher, which we have used for years. We consciously work to keep a wall to avoid conflicts and any appearance of impropriety between cases we have and those for codefendants or other conflicted Panel appointments.

For our CJA Panels, the Panel Selections Committees try to include lawyers with a wide range of trial and appellate/non-capital habeas experience, as well as diversity. Our Capital Habeas CJA Panel has a separate Selection Committee which also decides CJA capital habeas case appointments.

While we have had challenges in attracting diverse applicants, we generally have had enough Panel members to handle the cases the District receives. The only exception is for very large, multiple defendant cases or related cases – gang conspiracy or mortgage fraud. We are more challenged in finding capital habeas CJA counsel given the level of experience needed to these representations and that many of the these qualified lawyers already have full capital caseloads. The main factor inhibiting trial, appeal, and capital panel appointments is possible voucher cutting for work honestly performed.

Judicial intervention or blocking of CJA expert, investigator, paralegal, or other cost/budget requests is a factor, and sometimes an inhibitor to Panel

representation. Panel lawyers sometimes may second-guess a request and not ask, fearing denial and eventual voucher cutting.

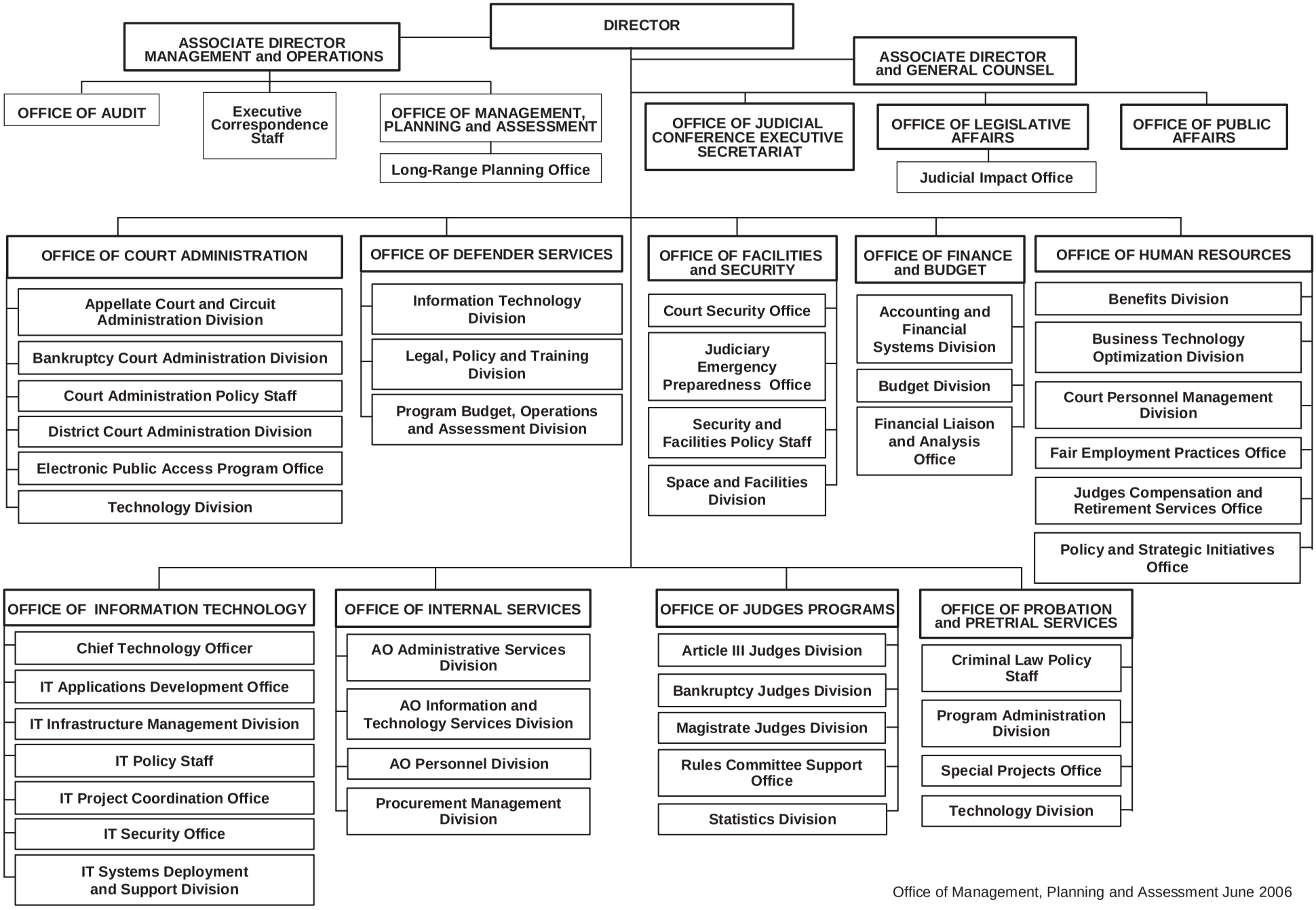
I have always thought it unfair that the lawyers fighting for due process for criminal defendants were themselves denied due process when a voucher would be cut, that these lawyers could not even go to the State Bar to mediate any disagreement in payment. A CJA voucher review panel in each district, consisting of a CJA Administrator, a CJA Supervising Attorney, a FDO attorney representative, and a private criminal defense lawyer from the community not on the Panel would provide a fairer review process for proposed voucher cuts.

Judges in our District sometimes call upon my Chief AFD, Branch Supervising AFD, or me to review vouchers a judge questions. One particular Panel attorney, known for high bills, especially when compared with codefendant counsel, had several bills questioned. That review revealed reasonable factors which should be considered in each case: differing ways of learning a case (some are more IT savvy versus paper dependent; aural versus visual; organizationally challenged, etc.). The particular Panel lawyer tried using an organizing paralegal, but had been burned by the paralegal's sudden abandonment and silence and left scrambling for deadlines and information; the lawyer was then loathe to risk being placed in that position again, trying to organize and investigate the case entirely on the lawyer's own. These situations are not always recognized by judges, so vouchers may be harshly cut.

Finally, we are proud of the CJA Panel training and support we provide these lawyers who are so dedicated to the 6th Amendment to accept these representations at less than market cost. We offer in both our Fresno and Sacramento offices monthly Panel trainings; topics range from ethics, bias, and substance abuse to forensics, new case, Guidelines, and statutory laws, successful techniques for certain cases, clients and at certain criminal process stages, and an annual Supreme Court review. We also publish a monthly

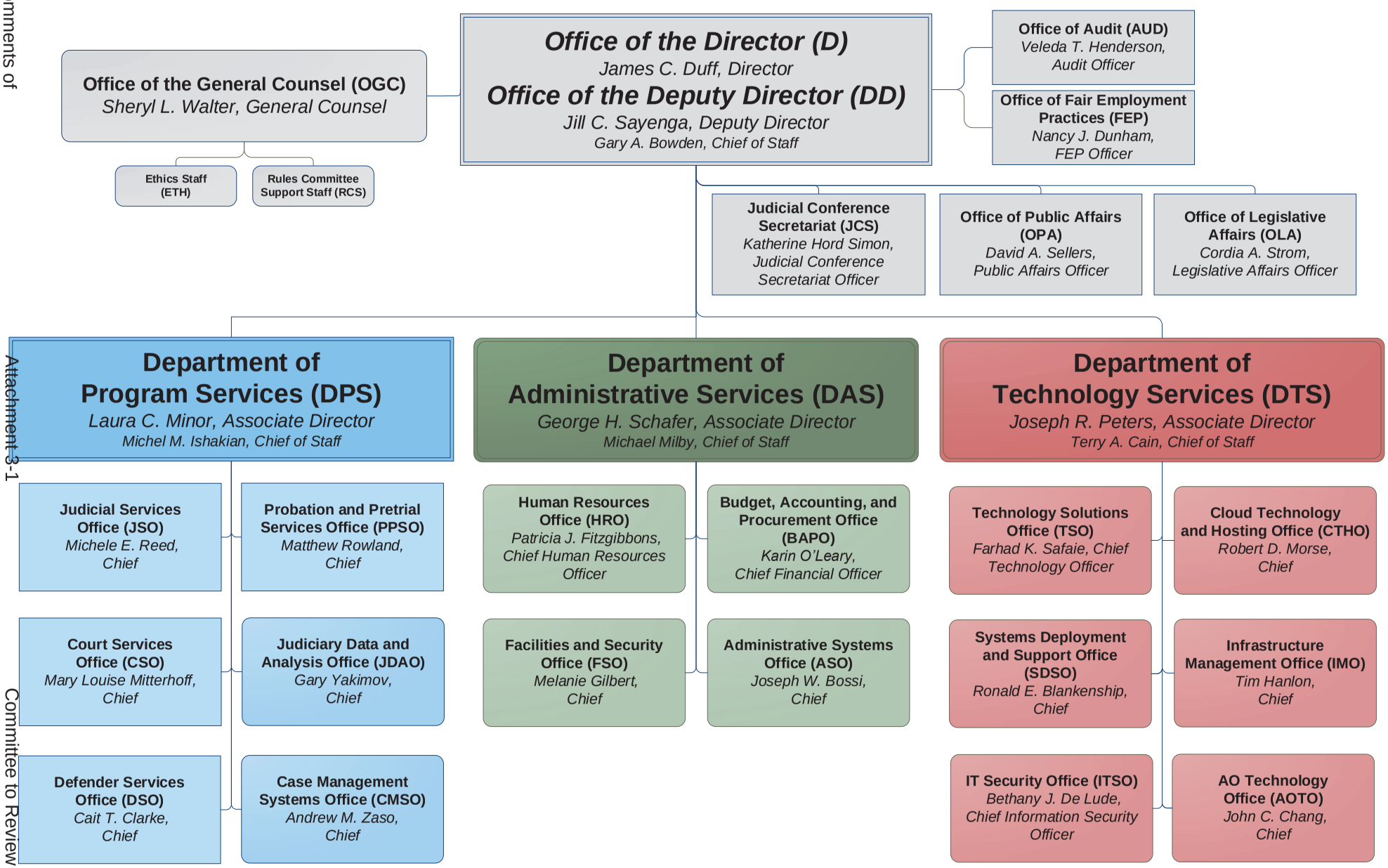
newsletter which includes changes in the law, trainings offered by our Office and the Federal Defender Training Branch, news in our specific legal community, and the CJA budget; I try to include each month a letter relevant or I hope interesting to our practice. The newsletter is sent electronically to our Office, the Panel, the Court, U.S. Attorney's Office, Probation and Pretrial, and is posted on our website. Hard copies are sent to local jails where our in-custody clients are housed.

Administrative Office of the United States Courts



Office of Management, Planning and Assessment June 2006

Administrative Office of the United States Courts



Administrative Office of the United States Courts

Department of Program Services (DPS)

Laura C. Minor, Associate Director
Michel M. Ishakian, Chief of Staff
202-502-3500

Judicial Services Office (JSO)

Michele E. Reed, Chief
Dan Jackson, Deputy Chief
202-502-1800

- **Judicial Policy:** *Michele E. Reed*
- **Judicial Programs:** *Dan Jackson*
- **Judicial Support:** *Fawne N. Lindsey*

Court Services Office (CSO)

Mary Louise Mitterhoff, Chief
Leeann Yufanyi, Deputy Chief
202-502-1500

- **Business Support:** *Leeann Yufanyi*
- **Operations:** *Gary E. McCaffrey*
- **Policy:** *Mark S. Miskovsky*
- **Programs:** *Robert Lowney*

Defender Services Office (DSO)

Cait T. Clarke, Chief
Rebecca A. Blaskey, Deputy Chief
202-502-3030

- **Administrative Operations:** *Samantha Wadkins*
- **Communications and Special Projects:** *Robin Maher*
- **Legal and Policy:** *Pamela B. Hamrin*
- **Program Operations:** *Stephen C. Macartney*
- **Training:** *Bob Burke*

Probation and Pretrial Services Office (PPSO)

Matthew Rowland, Chief
Nancy Beatty Gregoire, Deputy Chief
202-502-1600

- **Criminal Law Policy:** *John J. Fitzgerald*
- **National Program Development:** *Laura M. Baber*
- **Program Oversight and Support:** *Nancy Beatty Gregoire*
- **Training and Safety:** *Ronald L. Ward*

Judiciary Data and Analysis Office (JDAO)

Gary Yakimov, Chief
Catherine J. Whitaker, Deputy Chief
202-502-3900

- **Data Management:** *Shawnie Quigley*
- **Governance:** *Catherine J. Whitaker**
- **Reporting and Analysis:** *John Sporing Jr.*

Case Management Systems Office (CMSO)

Andrew M. Zaso, Chief
Frank B. Fuller, Jr., Deputy Chief
202-502-2500

- **Application Support:** *Douglas F. Quigley*
- **Business Support:** *Mario A. Lopez**
- **CM/ECF Next Generation:** *Margaret S. McCaleb*
- **Defender IT Support:** *John F. Fay**
- **Development:** *Peter Chin*
- **Project Delivery:** *Matthew E. Morris*
- **Release Management:** *Kathleen M. Ryan*

Note: Click on a box for additional contact information.

* As of this chart's revision date, this individual is leading the unit in an interim, acting capacity.

Department of Program Services

Defender Services Office (DSO)

Cait Clarke, Chief

Rebecca Blaskey, Deputy Chief

Program Operations Division

Mission
Provide budgetary and operational support for federal defender organizations (FDOs) and management assessments of FDOs and panel programs.

Develop, execute, and monitor defender services appropriation and financial plan, including detailed analyses of individual FDO budget and grant requests.

Perform on-site cyclical assessments of FDOs and panel programs with written reports and post-assessment coaching support to defender leaders and staff.

Manage case weighting studies for planning and budgeting purposes including support for current work measurement study.

Develop policy and provide guidance to FDOs relating to the Defender Compensation and Classification System (DOCS).

Administer grants to community defender organizations (CDOs) and develop and implement CDO-specific standards and policy guidance.

Legal and Policy Division

Mission
Support the Committee on Defender Services and its subcommittees and provide legal and policy guidance for the defender services program.

Prepare meeting agenda items, briefing papers, research and recommendations on a variety of legal, policy and funding issues.

Develop and communicate program policies and guidance through facilitation of advisory and working group processes

Research and analyze legal issues and recommend solutions in response to inquiries from federal defenders, panel attorneys, and courts.

Training Division

Mission
Provide training and conference support for defender staff and panel attorneys.

Design, implement, and teach national, local, and distance learning programs for panel attorneys and FDO attorneys, paralegals, and investigators.

Design, compile and manage content on online resource providing information, resources, materials and publications on federal criminal law and procedure, federal criminal defense practice.

Implement the Supreme Court Advocacy Program for panel and FDO attorneys representing Criminal Justice Act (CJA) - eligible defendants in the United States Supreme Court.

Provide advice, consultation, and training on electronic discovery and litigation support tools, service, and processes to FDOs and CJA panel attorneys.

Provide daily advice on criminal law matters to FPDs and panel attorneys.

Communications & Special Projects Division

Mission
Provide effective, coordinated, and timely communications related to all aspects of the program including communications with all members of the defender community, internal AO, and other judiciary entities. Provide project management direction and leadership, including short and long-range planning, budgeting, and resource allocation.

Develop processes and communications resources to ensure that all stakeholders are informed on essential issues associated with DSO.

Assemble and lead cross-functional teams from among DSO staff to address high-visibility and high-impact initiatives and projects of strategic importance to the program.

Defender Automation Coordinator

Contribute defender IT expertise in FDO operational policy development. Staff the Defender Automation Working Group (DAWG).

Facilitate and coordinate defender services IT activities with CMSO, DSO, and defender organizations.

Coordinate efforts with CMSO and DTS to ensure attorney-client protections are in place, periodically reviewed, and updated.

Coordinate with Program Operations, Legal and Policy, and Training Divisions on IT-related matters.

Administrative Operations Staff

Mission
Manage and support administrative infrastructure of DSO through process development and implementation and personnel assignments.

Budget support, analysis, and execution of DSO centrally-held funds and oversight of new decentralized budgeting process.

Manage federal defender staff security badges and official passports as well as visas for international case-related travel.

Overall administrative support for DSO divisions.

Travel authorization and reimbursement processing for DSO staff and federal defender travelers on program-related travel including training, assessments, and international prisoner transfers.

DSO correspondence and records management.

Knowledge management oversight including improving office-wide document collection, file organization and information access.

Written Comments of
FD-CAE Heather E. Williams

Case Management Systems Office (CMSO)

INTERIM

Andrew Zaso, Chief

Deputy Chief, Vacant

Project Delivery Division

Develop and implement consistent project management methodologies that enable CMSO to deliver high-value projects on time and within budget, and to establish best practices that encourage collaboration, standardization, and process improvement.

Project Management

- Manage all development efforts using the same project management methodology and procedures;
- Provide consolidated reporting on the status of all projects;
- Manage interactions with and expectations of DPS program offices and Department of Technology Services (DTS) Project Management Division;

Requirements

- Takes business requirements (User Stories) identified by stakeholders and defines them for use by a development team;
- Responsible for making sure non-functional requirements are defined for each system, e.g. system response time, system availability, back-up requirements, interfaces needs; and
- Works closely with the system architects to insure systems design follows best practices within the Judiciary.

Development Division

Perform a broad spectrum of duties to build software solutions to meet customer requirements and comply with enterprise and/or agency standards.

Solutions Architecture

- Determine the system architecture to be used for each application with consideration given to such things as centralized versus decentralized servers, use of service oriented architecture (SOA), and use of a single database versus individual databases for each court unit;
- Design non functional elements of each system e.g., response time, system availability, backup requirements, interfaces needs;
- Performs research into new technologies, products, standards which can be incorporated into CMSO applications as protypes;

Code Development

- Develop and maintain case management and related systems for federal appellate, district, and bankruptcy court judges and staff, probation and pretrial services officers, federal defenders, and external stakeholders;
- Design operational reports associated with applications;
- Design and develop software based on enterprise and/or agency standards; and
- Leverage best practices and code reviews to improve the quality of the software code.

Release Management Division

Facilitates the successful release of CMSO IT products to customers in the most efficient and effective manner with minimal disruption to customer operations. Partners with CMSO divisions, program offices, SDSO testing, training and support divisions, as well as customers to ensure delivery and adoption of high quality products.

Technical Documentation

- Partners with the program offices, CMSO divisions, and SDSO to create and deliver high quality documentation required to support the release and adoption of IT products.

Implementation

- Ensures product quality through configuration management and other quality assurance processes. Coordinates with program offices, CMSO divisions and SDSO to help customers prepare for product releases and assist in the successful adoption of IT. Coordinates release of products to production.

Internal Testing

- In coordination with CMSO divisions and the SDSO Testing Service Division, ensures product quality by making sure product functions properly with focus on internal functional and performance testing prior to deployment using efficient processes.

Application Support Division

This Division supports the application developed by CMSO after they are deployed to the user community. The Division is also responsible for maintain the development environment and tools used to develop the applications.

Issues Management (Tier III)

- Track issues which require CMSO staff resources to resolve;
- Work with the SDSO Support Division to respond to user requests for assistance that are escalated to Tier III;
- Ensure that solutions to issues are documented and shared with the SDSO Support Division in case they are needed in the future; and
- Build and maintain a knowledge data base to provide assistance to users and Court IT staff.

Environment Management

- Improve the quality of software development, deployment, and operations.
- Work with the CMSO Development Division to develop a consistent software building environment for all projects;
- Support and standardize development tools for use across CMSO;
- Work with other CMSO sub-offices to develop standard processes and tools for all projects; and
- Provide and maintain the server environments used for the development and internal testing of applications. This includes managing the Dev, Test, Pre-Prod, and Production environments.

Case Management Systems Office

INTERIM

Business Support and Communication Division

Support CMSO by providing the business support processes needed for the organization to be successful. These business processes include:

Financial

- Budget: Managing the operational budget of the office to include project funding through the different appropriations;
- Contract Management: Reporting on funding by contract, identifying renewals, working with the Procurement Management Division to manage acquisitions;
- Payment: Manage invoice payment;
- Ordering of supplies; and
- Ordering of equipment/software.

HR Functions

- Onboarding of new employees and contractors
- Performance appraisals for employees
- Recruitment of employees and contractors
- Separations of employees

Communication

- Weekly Significant actions;
- Special reports;
- Meeting minutes; and
- Preparation of responses to DPS, JC Committees, and working groups.

Travel

- Travel Authorizations.

Special Projects

Next Generation of CM/ECF Project Director

- Responsible for the delivery of Next Generation CM/ECF application to the courts.
- Work with stakeholders and working groups to define and prioritize requirements
- Collaborate with Development manager in the development of a delivery schedule
- Communicate with stakeholders on the progress of Next Gen CM/ECF

Portfolio Management Coordinator

- Work closely with other DPS offices and associated advisory groups to identify business needs and determine if existing applications in the portfolio meet those needs
- Work with stakeholders to estimate product development and life-cycle maintenance costs, and to define the functional and technical qualities of each product in terms of ROI to the Judiciary;
- Work with other CMSO sub-offices to ensure the products that are developed and deployed leverage existing applications developed within Federal Judiciary;
- Work with portfolio managers to ensure product interfaces are incorporated where viable and necessary to reduce the cost of ownership while maximizing effectiveness and efficiency; and
- Maintain an inventory of products in order to identify and eliminate redundancy, quantify the value of the products to the business, and improve the return on investment.

Defender IT Support

National Systems Information Management Branch

- DSMIS application management, change control, enhancements, testing, data quality assurance, user training, documentation, operations
- defenderData application management, change control, enhancements, testing, user training, documentation, operations
- Contract management associated with the above systems
- Develop defender data analysis tools and reports for use by DSO, Defenders, the AO, and the courts.

National IT Operations and Applications Development Branch

- Designs, manages, and supports the FDO centralized environment for delivery of e-mails and collaboration services to desktops and mobile devices.
- Designs, manages, secures, and troubleshoots the Defender Wide Area Network (DWAN) and all associated network equipment at the national data centers.

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