United States Department of Justice – Civil Division

Privacy Impact Assessment
for the
Civil Division

MEGANOC General Support System
and Mega Online Relativity Environment (MORE) Minor Application

Issued By:

Angie E. Cecil

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: February 15, 2019

EXECUTIVE SUMMARY

This PIA pertains to an information sharing system called MEGA Online Relativity Environment (MORE), which is part of a larger general support System named MEGA Network Operation Center (MEGANOC). These systems are designed to provide a seamless document review system for litigation support and facilitate collaboration among those working on cases handled by the Civil Division of the Department of Justice (Division). They were procured via the Mega 4 contract, an indefinite delivery, indefinite quantity contract vehicle available for use by the Department of Justice (DOJ) litigating divisions, including the Division. Under Mega 4, Leidos, a government contractor, provides managed hosting services which include a hosted web application from the MEGANOC, along with an alternate processing center. MEGANOC is a General Support System (GSS). The information system is managed by native Microsoft infrastructure components (e.g., Active Directory) collaborating with security management tools and an e-discovery application, Relativity. MEGANOC hosts large litigation support databases, document repositories, and a collaborative work environment to allow authorized Civil Division trial teams, other authorized individuals participating in the case, including experts, litigation consultants, client agencies, and co-counsel, to share the same set of case data. MORE is a minor application and a sub-system to MEGANOC, which allows MORE to inherit personnel and technical security controls. MORE's primary objective is to provide a seamless document review system for litigation support with a suite of tools for performing collaborative litigation review of case-related data. Users of the system are the same as MEGANOC users.

The Division completed this Privacy Impact Assessment (PIA) to review and document the Division's use of the MEGANOC GSS and MORE systems. (This PIA does not apply to other Department components' use of the systems.) The Division conducted the PIA to comply with the E-Government Act of 2002, the Federal Information Security Modernization Act, Department of Justice IT Security Standards and Security Authorization Process, and National Institute of Standards and Technology's NIST 800-53 Rev. 4.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system;
(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
(h) whether it is a general support system, major application, or other type of system.

The response should be written in plain language and should be as comprehensive as necessary to

describe the system. If it would enhance the public's understanding of the system, please include system diagram(s).

a) The purpose that the records and/or system are designed to serve:
MEGANOC hosts large litigation support databases, document repositories, and a collaborative work environment to allow authorized Division trial teams and other authorized individuals participating in the case, including experts, litigation consultants, client agencies, and co-counsel to share the same set of case data.

b) The way the system operates to achieve the purpose(s):
MEGANOC is a General Support System (GSS). The information system is managed by Microsoft infrastructure components (e.g., Active Directory) collaborating with security management tools and e-discovery applications.

c) The type of information collected, maintained, used, or disseminated by the system:
MEGANOC and MORE house data collected in the course of a Division investigation or litigation. This information may include information generated by the Division's client agencies and provided to the Division in support of an investigation or litigation. The information may be collected as part of a client-agency's investigation and provided to the Division or may be produced to the Division by an opposing party or third party in the course of the discovery process overseen by the federal courts.

d) Who has access to information in the system:
The information maintained in MEGANOC and MORE may be accessed by authorized Civil Division employees, other federal employees, and other approved personnel. Before access is authorized, the individual's access rights and purpose for accessing the documents is reviewed by the Civil Division's IT security staff. To this end, the Division places strict access controls via physical and electronic means in order to secure the information. For example, Division employees and contractors are only granted access to databases on the system that support a matter they are working on. Databases are case specific. If an employee or contractor leaves or is reassigned, the account access is disabled or access to a particular database may be rescinded.

e) How information in the system is retrieved by the user:
The user retrieves the information in the system via a web browser search form that permits keyword searches applied to specific datasets for the case or matter the user is authorized to access. The search tool provides the capability through the web form; users search data across the case database by using the searches using related keywords such as custodian names, dates, or any relevant information associated with the case or matter. The system will display the retrievable results in a web response message.

f) How information is transmitted to and from the system;
The information is transmitted to the system from the Division via encrypted external hard drives which will be hand carried to the MEGANOC operation center and processed to store in the SQL database system with encrypted storage. The information is queried via a secured web

request from the user interface, then the data is transmitted electronically through secured authorized access to the web interface.

g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):
MEGANOC GSS is a self-contained contractor-owned and operated system that does not interconnect with any DOJ systems. The case information originates from the Division via encrypted external hard drives which will be hand carried to the MEGANOC operations center to load into MORE and later retrieved via a secure web interface. However, the MEGANOC environment resides in a shared service infrastructure that connects to other contractor-owned and operated systems. MORE is a sub-system to MEGANOC inheriting infrastructure, security, and monitoring controls from the parent system.

h) Whether it is a general support system, major application, or other type of system.
MEGANOC is a general support system and MORE is minor application.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration	X	Financial account	X
Taxpayer ID	X	Driver's license	X	Financial transaction	X
Employee ID	X	Passport	X	Patient ID	X
File/case ID	X	Credit card	X		
Other identifying numbers (specify):					

General personal data					
Name	X	Date of birth	X	Religion	X
Maiden name	X	Place of birth	X	Financial info	X
Alias	X	Home address	X	Medical information	X
Gender	X	Telephone number	X	Military service	X
Age	X	Email address	X	Physical characteristics	X
Race/ethnicity	X	Education	X	Mother's maiden name	X
Other general personal data (specify):					

Work-related data					
Occupation	X	Telephone number	X	Salary	X
Job title	X	Email address	X	Work history	X

Work-related data					
Work address	X	Business associates	X		
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	
Palm prints	X	Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures	X	Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run	X	Contents of files	
Other system/audit data (specify):					

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax	X	Online	X
Telephone		Email	X		
Other (specify):	Documents are obtained through litigation discovery				

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign	X		
Other (specify):					

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	X
Commercial data brokers					
Other (specify):					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats

to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

As described above, the information managed on MEGANOC GSS and MORE is provided to the Division in the course of litigation. The documents are typically provided by another DOJ component or another federal or state entity involved in the investigation. The information may also be received from an individual if the Division is handling the representation of the individual. Other information may be provided by the opposing party or third party in the litigation in response to a subpoena or other discovery request. The privacy risks associated with collecting records from other entities is that they will share information outside the scope of the investigation or not properly identify the data being ingested into the system as containing personally identifying information. Preventing the exposure of the data once is it received by the Division minimizes the risk that personal information will be shared outside the team of individuals working on a particular matter. To this end, the Division places strict access controls on MEGANOC and MORE via physical and electronic means to secure the information. For example, Division employees and contractors are only granted access to databases on the system that support a matter they are working. If an employee or contractor leaves or is reassigned, the account access is disabled, and access to a particular database is rescinded.

The system is also configured with multi-factor authentication. This requires all authorized end users to provide two levels of authentication prior to accessing any data hosted on the system. Users may also request access to multiple databases and are required to go through the request process for each database they wish to be authorized to access. The system is configured to ensure that access to a specific database and its content is restricted to only those users that have authorized access. The system is also monitored and audited to identify any unauthorized access attempts and to verify that the appropriate access level have been granted to its users. The system is hosted behind security firewalls and intrusion detection systems. All the data resides on encrypted storage, and the websites are secured behind a firewall which requires proper authentication and authorizations to the website. The data transmissions are also encrypted using secure protocols (i.e., SSL/TLS & HTTPS). This ensures that all data transmissions are protected.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities	X	For civil enforcement activities
	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
X	For litigation		
	Other (specify):		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The Division's litigation mission includes civil and criminal enforcement. Sensitive but Unclassified data is stored in MEGANOC and MORE. The information collected is used to accomplish activities inherent in the Division's investigations and litigation, including: reviewing documents for relevance to claims and defenses; conducting privilege reviews of documents collected in the investigation; tracking the use of documentary evidence in litigation; preparing witness kits/binders for depositions and hearings; geospatial and link analysis relevant to litigation or investigation; and selecting and preparing exhibits for trial. Collection, maintenance, and use of the information supports the Division's litigation and administrative functions.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	28 USC §§ 514-19
	Executive Order	
X	Federal Regulation	28 C.F.R. §§ 0.45-0.49, Subpart I
	Memorandum of Understanding/agreement	None (not established)
X	Other (summarize and provide copy of relevant portion)	DOJ Contract #DJJ07-C-1523 ("Mega3 ALS") for automated litigation support services.

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Data will be retained in the system until the Division case attorney and the Office of Litigation Support determine that the litigation materials no longer need to be stored. Information no longer needs to be maintained after a case has closed, settled, and the information is not needed for other cases or investigations. In consultation with the attorney assigned to the matter, the Office of Litigation Support will dispose of data that does not need to be maintained pursuant to the Division's obligations under the Federal Records Act. Information that must be maintained will be retained in accordance with the applicable retention schedule. Data will be disposed of after consultation with the case attorney. Archiving a case leaves the data with the attorney and available in another format or location for the attorney to access in the future. The space previously utilized by the case in MEGANOC and MORE is re-used (deleted, then made available elsewhere).

Files managed on MEGANOC and MORE may include both federal records and non-records that are associated with a variety of different types of Division's litigation case files. The retention policies for the files depend on the federal record status as well as the classification of the type of case file to which the files pertain. The DOJ record retention schedules are published at (https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0060. Record retentions for case files range from approximately 5 years to 65 years after the case closure date. Temporary records are destroyed at the end of the retention period, and permanent records are transferred to the custody of the National Archives and Records Administration. Non-records, such as duplicates and unnecessary discovery or other submitted documents, are destroyed when no longer needed.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There is a potential risk to privacy that could result from the improper access to information in the system; however, security protections that authorize and limit a users' access to information within the system mitigate the risk. Physical controls such as secured entrances and security officers protect access to the building where the servers and workstations are located. DOJ approval is required before a user can access the system. The authorized users will be provided with multi-factor authentication mechanism to access the system. The user is required to complete required security training, including cybersecurity training and privacy training, as well as to annually acknowledge the applicable rules of behavior. Individuals outside the Division are required to sign a confidentiality agreement and rules of behavior documents before they are provided with access accounts. In addition, all contractors granted access to the system must adhere to the Department's IT security standards for reporting security incidents.

Information access to the system is granted on a need to know basis. For example, Division attorneys, other staff members, other federal employees, and contractors are only granted limited access to the matters they work on, not the entire system. There are monitoring

and auditing tools for each system to review user activity, so Leidos (contractor) can monitor user access within the system. Leidos is the only contractor involved in the management of this system. The contractor follows DOJ policies and procedures for unauthorized access or release of information from the system. Additional information regarding cybersecurity protections are discussed in the last paragraph of Section 4.2 below.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X		X	
DOJ components	X		X	
Federal entities	X		X	
State, local, tribal gov't entities	X		X	
Public				
Private sector			X	Contractors to the department
Foreign governments				
Foreign entities				
Other (specify):			X	Opposing counsel

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Security protections that authorize and limit a user's access to information within the system mitigate the risks to privacy. Unauthorized physical access to the MEGANOC system and MORE application is limited by physical controls such as secured entrances and security officers. The data maintained by the MEGANOC system and MORE application is protected through compliance with the Department's access control policy. To access the system, the Division enforces Department standards for accessing a network system, such as contractor badge reader card entry and role-based access controls. To access the system, DOJ prior approval is required. The authorized users will be provided with multi-factor authentication

mechanism to access the system. The user is required to complete required security training, including cybersecurity training and privacy training targeted, also rules of behavior acknowledged annually to the user's role. Individuals outside the Division are required to sign a confidentiality agreement and rules of behavior document before they are provided with access accounts. In addition, all contractors granted access to the system must adhere to the contractor's and DOJ IT security standards for reporting security incidents. For data in transit, the contractor utilizes DOJ-approved encryption technology.

Information access to the system is granted on a need to know basis. For example, Division attorneys, other staff members, other federal employees, and contractors are only granted limited access to the matters they work on, not the entire system. There are monitoring and auditing tools for each system to review user activity, so that Leidos can monitor user access within the system. The contractor follows DOJ policies and procedures for unauthorized access or release of information from the system. For data sets that contain particularly sensitive information, the folder access provides an audit trail in the MORE application.

The MORE application and MEGANOC system security plan, including administrative and technological controls, is documented in accordance with DOJ procedures. MEGANOC exists on a physically secure, environmentally protected, non-DOJ, corporate network protected by firewalls, and is administered by DOJ-cleared contractor personnel. MEGANOC's, and subsequently MORE's, connection to the Internet is firewall protected and communications to and from the server are encrypted via SSL/TLS. The MEGANOC firewall and operating system security are tested monthly. Patches are applied according to the DOJ Configuration Management Plan and the DOJ Vulnerability Management Plan to maintain system security. MEGANOC access is monitored by inspection of event logs, system logs, web logs, database application logs, and firewall logs. Access to MEGANOC is granted only to DOJ-approved individuals who have signed a confidentiality agreement and system rules of behavior. Access to specific databases is granted on a need to know basis by user account and password. All MEGANOC GSS accounts are "named user" accounts assigned to a single individual. A documented process exists for requesting, granting, and reviewing account activity, and terminating accounts. As account requests are reviewed and denied or approved, and accounts are terminated, these actions are recorded in the MEGANOC GSS Status Report Spreadsheet to DOJ Civil Division Office of Litigation Support.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:

	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Documents are obtained through court order, warrant subpoena, and other such legal means. In the context of adversarial proceedings, such as an investigation or litigation, consent, access, and amendment protections are not applicable to the records. An opposing party may challenge the relevance of the information and not produce the information in litigation, but that challenge would be determined before the information is collected and maintained by MEGANOC. For social media captures and web site collections, notice is not provided to individuals as the information is considered to be in the public domain.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:

X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Documents are obtained through court order, warrant, subpoena, discovery requests, and other such legal means. In the context of adversarial proceedings, such as an investigation or litigation, consent, access, and amendment protections are not applicable to the records. An opposing party may challenge the relevance of the information and not produce the information in litigation, but that challenge would be determined before the information is collected and maintained by MEGANOC. For social media captures and web site collections, notice is not provided to individuals as the information is considered to be in the public domain.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Unless individuals are opposing parties in litigation, individuals do not provide information directly to the Division for use in MEGANOC and MORE. In the context of adversarial proceedings, such as an investigation or litigation, consent, access, and amendment protections are not applicable to the records. Individuals who are opposing parties in litigation can object to the Division obtaining the information through the discovery process. Individuals whose information is collected in the course of litigation involving another entity, such as another government agency or business entity, may have the opportunity to consent at the collection from the other entity. If another government agency is involved in the investigation or litigation, the agency's System of Records Notice would provide notice that the information may be shared with the DOJ for the context of a civil or criminal investigation or litigation. For information collected from the internet, notice is not provided to individuals as the information collected is in the public domain.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: Megan - ATO - 5/12/2017 & MORE - ATO 01/05/2019 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:	
X	A security risk assessment has been conducted.	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Completed FISMA Moderate risk evaluation via DOJ Security Authorization Handbook.	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Completed DOJ Security Authorization, and continuously monitor applications and web sites for misuse. Perform ongoing security scanning with commercial off-the-shelf (COTS) product Tenable Nessus Vulnerability Scanner. This tool provides the capability to assess compliance and vulnerability standards against security benchmarks.	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: This system satisfies the Audit and Accountability (AU) controls outlined by NIST 800-53A-Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, including formalized Audit and Accountability Policies and Procedures, technical controls, and role-based privilege separation. All approved policies, procedures, standards, and program plans fully meet the requirements of FISMA. User activity audit logs are maintained in the MEGANOC system.	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
	X	Training specific to the system for authorized users within the Department.
	X	Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

The MORE application and MEGANOC system security plan, including administrative and technological controls, is documented in accordance with DOJ policy. MEGANOC exists on a physically secure, environmentally protected, internal network protected by firewalls, and is administered by DOJ-approved, contractor personnel. MEGANOC's connection to the Internet is firewall protected and communications to and from the server are encrypted via SSL. MEGANOC firewall and operating system security are tested monthly. Patches are applied as appropriate to maintain system security. MEGANOC system access is monitored by inspection of event logs, system logs, web logs, database application logs, and firewall logs.

Access to MORE application MEGANOC is granted only to DOJ-approved individuals

who have signed a confidentiality agreement and system rules of behavior. Access to specific databases is granted on a need to know basis by user account and password. All MEGANOC accounts are "named user" accounts assigned to a single individual. A documented process exists for requesting, granting, and reviewing account activity, and terminating accounts. As account requests are reviewed and denied or approved, and accounts are terminated, these actions are recorded in the MEGANOC Status Report Spreadsheet to DOJ Civil Division Office of Litigation Support.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: JUSTICE/CIV-001, *Civil Division Case File System,* last published in full at 63 FR 8659, 665 (Feb. 20,1998), https://www.gpo.gov/fdsys/pkg/FR-1998-02-20/pdf/98-4206.pdf.
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information specifically pertaining to US citizens and/or lawfully admitted permanent resident aliens can be retrieved from the system, but is handled in strict accordance with all Federal regulation regarding PII and Sensitive but Unclassified material. MEGANOC and MORE offers a variety of retrieval solutions, which generally allow a full-text or fielded search on document data and metadata collected (e.g. date sent, from, to, cc as collected or produced via the discovery protocols). A full-text search uses the database's index to quickly sift through every word (of every record) that can be entered in the database. A fielded search permits the user to narrow the dataset to be searched within a matter to particular fields, sets, or data. For both searches, the user can search and retrieve a list of documents and then view the documents found by the search. First party's access to personal information retrieved in the system and potential amendment rights are controlled by the SORN listed above and may be covered by 5 U.S.C. § 552a(d)(5).