DISA OFFICE OF THE GENERAL COUNSEL'S DEPARTMENT OF DEFENSE ENTERPRISE EMAIL (DEE) SEARCH GUIDE

Current as of 23 January 2017

Contents

What's New:

Section/Page/Paragraph	*Change made*
1, paragraph 2	Included "records professionals" in target audience for Guide
1.1, paragraph 1	Clarification of "ownership" of emails
1.3	Definitions added: DISA DEE LECI Support; Business Class Accounts; Journaling/Journaled Accounts
3.6	Added recommendation to litigators re: records professionals
4.1.1, paragraph 2	Added requirement for group email boxes
4.1.1	Clarify example in second paragraph
4.1.1	New 5th paragraph
4.4	Added requirement for requester to access search results within 14 days
5.1	FOIA requests now only require approval of the FOIA officer's attorney if the FOIA asks for legal office files, otherwise, the FOIA officer may make the requests (accompanied by a copy of their letter of appointment as the FOIA officer), but without an accompanying statement from a servicing attorney.
5.1.1	Clarification on "electronic signatures"
5.2.1	Clarification on "electronic signatures"
5.3.1	Clarification on "electronic signatures"
5.4	Removed requirement for a requester's attorney review of the requested documents. Added requirement for request to be made or endorsed by the first O-6 or GS-15 in the target account holder's chain of command.
5.4.1	Clarification on "electronic signatures"
5.5.1	Clarification on "electronic signatures"

Special thanks to Air Force Records Office –SAF/CIO A6XA
for helping to improve this Guide.

If you have suggestions for improvement, please email

DISA DSCC EIS Mailbox Cols-LECI Requests
<disa.dscc.eis.mbx.cols-leci-requests@mail.mil>
or
DISA DSCC OPC Mailbox COLS LECI Requests
<disa.dscc.opc.mbx.cols-leci-requests@mail.smil.mil>

DEE Search Process

Save time by sending complete documentation (see Guide)

1. Mission Partner defines scope of search (what account(s) to search, what search terms, what time frame, appropriate supporting documentation) and submits the request

DEE emails only @mail.mil or @mail.smil.mil

2. DISA Defense Enterprise Email (DEE) LECI Support group in-processes all requests and routes within DISA

DISA DEE LECI Support group will confirm by email

3. DISA OGC confirms documentation sufficient

Search time cannot be estimated

4. Search queued into DEE System

Designated recipient must be government personnel (civilian or military)

5. Search Results uploaded to secure sites

6. Requester emailed instructions for downloading

Requesting organization is solely responsible for release decisions

1. Introduction

This DISA Office of General Counsel (OGC) DEE Search Guide is designed to help Department of Defense (DoD) Enterprise Email (DEE) Mission Partners navigate the process for requesting DEE email searches and get the most out of search results.

This Guide is intended to help non-technical personnel—investigators, attorneys, records professionals, Freedom of Information Act (FOIA) officers, and others—understand how to request searches of the DEE system. This is not a technical document—if you need technical details about the DEE system, please contact your organization's Engagement Executive in DISA's Mission Partner Engagement Office (BDM) (see http://www.disa.mil/Computing/Engagement-Executive .

This Guide discusses what can be searched, what can't be searched, who can request a search, documentation required, how search results are delivered, and Frequently Asked Questions (FAQ). To make it easier to find the instructions you'll need to make a request, we've organized this version of the Guide by the function of the Requester—FOIA, Investigations, Litigation, NARA Archiving, and Other.

We recommend you review the contents of this Guide, even if you've been using the previous version—a lot has changed in the past couple of years and we've tried to streamline the process.

1.1. Legal Status of DoD Enterprise Emails and System

DISA Office of General Counsel (DISA OGC) has determined that DEE emails belong to the DEE Mission Partner provisioning the account—that is the MILDEP, Command, Agency, or other DoD organization paying for a particular user's DEE account—not DISA. DISA is itself a DEE Mission Partner, but we only "own" those emails being generated by accounts that we provision for our own personnel. In other words, DISA has physical custody of the emails residing in DEE, but the DEE Mission Partner still has legal custody.

As currently configured, the DEE system is not a system of records and DISA is not the Records Custodian for DoD emails. Email retention and preservation policies are set and executed by DEE Mission Partners, not DISA. Furthermore, DISA neither sets nor enforces acceptable use standards for email use by DEE Mission Partners.

Because DEE emails belong to the Mission Partner, DISA will provide access to emails only to authorized personnel. ***Search warrants, court orders, and subpoenas are not required.*** Any provisioning organization may request a search of its DEE accounts and we will provide the search results according to the process described in this Guide. Investigators with sufficiently documented authority may also request email searches.

Please note: For non-DoD organizations, such as FBI or DoJ, we ask that the search request come from the relevant DoD Command or Component. The search request must comply with the requirements discussed below, but will not require a court order or other authority.

When DISA performs a search for DEE emails we do not review or read the actual emails in the search results. ***DEE Mission Partners, therefore, are responsible for reviewing all search results and making all release determinations.*** This includes release of emails and attachments under discovery orders, FOIA requests, Congressional inquiries, etc.

DISA OGC does not provide legal guidance to DEE Mission Partners. This means that each DoD organization requesting a DEE search must seek legal guidance from its own legal counsel. Each DEE search requester is responsible for obtaining the legal reviews or approvals required by their Command or Component's chief legal counsel. When in doubt, contact your local legal office for assistance.

1.2. Expectation of Privacy and Information Security

All DoD personnel are given notice, by banners and user agreements, that system use (including the DEE System) is subject to monitoring and, by using DoD systems and equipment, each user consents to monitoring, including use of the DEE System for sending and receiving emails and attachments. ***Individual users have no expectation of privacy when using the DEE system to send or receive messages, including attachments.***

Nevertheless, DEE Mission Partners (provisioning organizations) do have a security interest in the information that their users send or receive through the DEE system. Mission Partners will appoint staff known as "Trusted Agents," who will be authorized by them to request email searches and review the results. Therefore, DISA only responds to requests and provides email search results to Trusted Agents and other Government entities with a legitimate requirement) who have documented "need to know" and have authority to request searches and receive results.

DISA understands that contractors provide valuable support to DoD, but as a matter of policy, we will only accept searches from government personnel (military or civilian) and will provide access to search results only to government personnel.

1.3. Definitions

These definitions apply to this Guide and DEE search requests—they are not meant as technical specifications.

Term	Definition/Comment
DEE Service Class	DEE provides five levels of mailbox service (see section 3.2): • Basic Class with a 512MB mailbox • Business Class Service* with a 4GB Mailbox online Exchange Mailbox • Premium Class Service* with a 10GB online Exchange Mailbox • Executive Class Service* with a 30GB online Exchange Mailbox • Senior Executive Class Service* with a 50GB online Exchange Mailbox User can delete or move emails out of the Inbox and out of the DEE System (which means they won't show up in a DISA mailbox search). Mailboxes of Journaled end-users are preserved and can be searched.
DEE Mission Partner	The organization provisioning DEE accounts (e.g., MILDEP HQ, Command, Agency); not to be confused with the "user" (individual).
Department of Defense (DoD) Enterprise Email (DEE) System	DoD's Enterprise Email infrastructure service operated and managed by DISA, includes enterprise-level software and hardware.
Digital signature	Unique identifying information resident on CAC card and applied to emails, Word documents, .pdf files, etc., to prove identity of sender or signer.
DISA DEE LECI Support	DISA DEE LECI Support, the office within DISA's Enterprise Service Directorate that in-processes all DEE search requests. Their email address is disa.dscc.eis.mbx.cols-leci-requests@mail.mil .
Email	Includes header, subject line, text of message, attachments; "owned" by the DEE Mission Partner, not DISA.
Encryption/ Encrypted email	DoD uses Public Key Infrastructure to encrypt or "lock" emails. DISA cannot open encrypted emails and only the header of encrypted emails can be searched.
Enterprise	Federation Constitution-class Cruiser, captained originally by Starfleet Captain Christopher Pike. Also refers to the entire DEE system, as opposed to regional PODs.
Exchange	Microsoft Enterprise-level email software

Expectation of privacy Privacy interest	Does not apply to DEE emails—individual users have no right to privacy when sending or receiving emails on the DEE System, even if the emails are going to or from a non-DEE system. Contact your organization's legal counsel for guidance.
Header	Technical term for the top part of every email in the galaxy – it includes the subject and sent/received information that cannot be changed; not usually visible to users, it contains the metadata of the email message.
Journaling Service Journaled Account	An optional service that captures all emails sent and received; even if the user deletes a message from his/her Inbox it will still show up in a search; see Section 3.3; may be used for Capstone approach to records management of email from the National Archives and Records Administration (NARA).
Local drive	A user's laptop or workstation which may contain emails copied from DEE into a .pst file. DISA can't search local drives.
Outlook	The Microsoft client (local machine) software used to read, compose, and manage emails and attachments.
Outlook Web App OWA	Web-based version of Outlook; CAC is required to use and access DEE emails.
POD	PODs are self-contained systems with the technology to deliver DEE services for up to 75K mailboxes. These are located at designated DECCs.
Preservation	Temporary hold of target account so that emails are retained by System and cannot be deleted by the user; by default DISA runs "searches" not "preservations"
.pst file	The type of file that Microsoft Outlook uses to store emails and attachments on a local drive. DEE search results are delivered in a .pst file created for each search.
Requester	Government POC submitting a request for a DEE search – this is ***not*** the same as a FOIA requester.
Search	Querying of DEE System for emails and attachments matching criteria (account, date/time, key words, recipient, etc.) supplied by the Requester
User	DoD personnel who have a DEE account to send/receive emails; the accounts are provisioned by the DEE Mission Partner organization.

2. Frequently Asked Questions (FAQs)

Question	Answer
Who can request a search?	Mission Partner "Trusted Agents" and Government entities with a legal requirement; they must be authorized to request and conduct email searches..
How do I request a search?	Send a request to DISA DEE LECI Support. See Section 5 for details.
When will my search results be available?	We don't know. It depends on the complexity of the search and the availability of system resources. But we will contact you as soon as results are ready for download.
How long does it take for a search to be queued into the System?	It depends on the volume of incoming requests. Allow at least 72 hours between the time we get a complete search request and the time a query is keyed into the System.
How do I get a status of my search request?	If DISA DEE LECI Support has confirmed receipt of your request, rest assured that we will let you know when results are available. But if you need to know the status, send an email to DISA DEE LECI Support – be sure to include the DISA Search number.
How will I get the results of my search request?	We will send you a link and instructions to access a secure site.
How do I make a preservation request?	By default all requests are *search* requests. If you really, really need a *preservation* instead, please follow the guidelines for Investigations or Litigations and include a justification for preservation. Typically, we will send the search results to the requester for the requester to preserve.
What is a Journaled account?	A journaled account is an optional DEE service that provides Mission Partners the ability to retain all messages and their attachments sent to and from selected journaled mailboxes. While not required for all end-users, it is recommended for high ranking and other designated individuals whose email is part of an official record and is subject to legal and regulatory requirements. Journaled accounts are preserved for 10 years.
Can DISA search for attachments to	Yes and no. The System treats most non-

emails?	encrypted attachments as part of the message itself. So we can search some attachments, but not whether there *is* an attachment. See para 4.5 for more information.
Can DISA search non-encrypted but password-protected attachments?	No.
Who decides whether an account is journaled or not?	The provisioning organization makes that determination; journaling can be provisioned when an end-user account is set up, or as needed. (journaling is not retroactive, it begins once the journaled account is created).
Can my organization make all of its user accounts journaled accounts?	Yes, if necessary, but it's going to cost you a lot more for each account (because there will be extra storage costs).

3. Summary of the DEE System

DISA was directed by the DoD Chief Information Officer to build DoD Enterprise Email, a service that provides secure email to the DoD enterprise that is designed to increase operational efficiency and facilitate collaboration across organizational boundaries. As an enterprise-wide service, DEE reduces the cost of operations and maintenance by consolidating hardware into DISA's secure, global Defense Enterprise Computing Centers (DECCs) via self-contained units called PODs, where Mission Partner mailboxes are located.

DEE creates a scalable common platform for the DoD (able to support 4.5 million users and 10 million mailboxes for CAC personas and non-person entities), ensuring Agencies can easily and effectively share information among virtual groups that are geographically dispersed and organizationally diverse.

> NOTE: Continuity of Operations: DEE adheres to the Federal Continuity of Operations Plan (COOP) initiative and Disaster Recovery Plan (DRP) requirement. DEE design provides redundancy both locally and remotely for all components of the system, replicating data between paired sites to facilitate continuity of operations/failover in the event of a catastrophic failure.
>
> DEE is implemented at DISA DECC locations throughout the world; POD locations are selected to provide optimal service and performance. These sites are strategically paired to provide failover, with each site having the capacity to support the primary instance and paired site in the event of a failover situation. Data is continuously replicated from the primary site to the paired site via dedicated Internet protocol security (IPsec) virtual private network (VPN) tunnels. This design allows DEE to provide this service with 99.9% availability.

3.1. Types of DEE Accounts

Currently there are five types of DEE user accounts plus an optional journaling service that can be assigned to any mailbox. DEE Mission Partners determine the type of account for each end-user when the account is provisioned and can change the type using the DEE provisioning portal. The type of account (service class) determines the amount of storage available:

- Basic Class Service with a 512MB mailbox
- Business Class Service* with a 4GB Mailbox online Exchange Mailbox
- Premium Class Service* with a 10GB online Exchange Mailbox
- Executive Class Service* with a 30GB online Exchange Mailbox
- Senior Executive Class Service* with a 50GB online Exchange Mailbox

* Journaling option available.

NOTE: End-users are responsible for keeping their mailboxes to an optimal size and will receive warnings as they approach their account maximum.

All classes of DEE mailboxes are accessible for search and hold requests. That said, end-users are able to self-archive and delete email from their mailboxes (this is part of how an optimum mailbox size is maintained). Such mail remains on the DEE servers for up to 14 days, even if "permanently deleted"; email in the 'Deleted Items" folder may be overwritten by DEE after 60 days.

NOTE: Journaled end-users may delete content from their regular DEE mailbox, but the journaled mailbox retains ALL email and attachments that were sent and received for up to ten years. Searches will include both regular and journaled mailboxes.

3.2 Deprovisioned Accounts

Each email sent or received by a DEE account user exists in the System as long as it is tied to an existing user account and isn't deleted or moved out of the System.

Deprovisioned accounts are accounts that the DEE Mission Partner organization has canceled using the DEE account management portal, or through automatic updates of the CAC system. DEE Mission Partners are advised that when an account is deprovisioned, the System is likely to overwrite the account and all associated data in 120 days. *This means that after 120 days all emails for the deprovisioned/deleted account probably cannot be searched or retrieved by the user or under a DEE search request.*

The way the System handles deleted accounts is subject to change according to DEE policy and storage requirements and limitations. Requesters are advised to submit requests for email searches when needed, regardless of whether the target accounts have been canceled or deleted.

3.3 Deleted Emails

There are two ways that an email can be deleted from the DEE System:

- User soft delete: the email will be moved by Outlook from the user's Inbox to the user's Deleted Items folder; the email still exists on the System and can be searched and retrieved for approximately 14 days;

- User hard delete: if the user "hard deletes" the email (empties the Deleted Items folder in Outlook), then the email will remain on the System overnight.

Please remember:

DISA never deletes emails, but a user can and the System will use all available space, so it will automatically overwrite any emails in a deprovisioned or expired account.

Journaled emails are kept for 10 years, even if the DEE account is deprovisioned.
It is the Mission Partner's responsibility to have a federal records management plan, including transfers of specified data to National Archives and Records Administration

3.4. Emails Moved to Local Storage

Because all accounts have storage limits on the System, many users will copy emails out of the System into local .pst files. These are files set up by the users or their local technical support and DISA *cannot* search them.

Litigators and investigators should contact their local network or system administrators for assistance in searching local machine drives. **Depending on the DEE Mission Partner's internal processes, litigators may also contact their records professionals for assistance.**

4. General Information about Searches

4.1 What DISA Can Search for

DISA can search for any emails on the System from when the Mission Partner began using DEE to the present. We can search any account that ends in @mail.mil or @mail.smil.mil. For other accounts, please contact your local network or system administrator for assistance.

Each search has three parts: target account(s); date range(s); keyword(s).

4.1.1. Target Accounts

Just because an email address appears in the Global Address Listing (GAL), doesn't mean we can search it. DISA can only search DEE accounts—that means email addresses ending in @mail.mil or @mail.smil.mil.

DISA cannot look up accounts; they must be provided by the requester (the authorized Mission Partner Trusted Agent or Government entity). A search may be for one or more target accounts. We need the name associated with the account ***and*** we need the email address. For a DEE organizational mailbox or group email box, this is the name of the mailbox and its email address.

Each target account must belong to the requesting organization or fall within the investigative authority of the requesting organization. For example, a request for search of Starfleet Academy target accounts coming from the Klingon High Counsel's FOIA office will be denied—Starfleet Academy owns the accounts and must request the search.

4.1.2. Date Range

Most searches include a date range, which will limit the search results. Because this search process is DEE specific, the date range can be as early as when the end-user's DEE service began; we can't search for emails prior to migration to DEE. Because the DEE System spans many time zones, we use GMT/ZULU by default. If your request is asking for a very narrow date/time range, we recommend you specify GMT to ensure accurate results. For best results, consider adding a day on either side of the date range.

A date range is not required, so we can search "from account creation to present." A search without a date range will yield more results, so requesters are advised to consider using a date range to narrow the results, when possible.

4.1.3. Keywords or phrases

Keywords and phrases are not required, but search results can be narrowed by including them in the search criteria. Requesters should consider carefully—only emails with exact matches will be in the results.

In addition, only the headers (which includes the subject lines) of encrypted emails can be queried, so if the keyword or phrase isn't in the subject line, the encrypted message won't be in the results.

DISA will not interpret search requests, so any keyword lists should include all acceptable permutations of the keywords or phrases. For example, if you request a search for the "Ferengi Rules of Acquistion", your search results won't capture an email with "Ferengi Rules of Acq." or "the Ferengi Rules." Instead, you should consider requesting "Ferengi" or "Ferengi Rules" or "Rules of Acquisition" as your keywords.

Requesters can always apply keyword criteria to the search results that the System generates. Search results are delivered in the form of a .pst file set up for the particular request. This means that the requester can search the search results in Outlook. This may be helpful for investigations or broad discovery requests which may require ongoing narrowing of search criteria.

4.2. What We Can't Search for

4.2.1. Transaction or Logging Data

DEE retains log-in data when a user's Outlook logs into the DEE System to upload or download emails, etc. This data relates to the Outlook-DEE System connection, not to the user's local log on. The System does not track when a user logs out because that is done locally, not on the System. The amount of logging data is vast, so it is not retained for more than about 10 days and it is used for System performance measurement, not for auditing user activity.

DISA does not currently have the hardware or software required to search the logging data collected by the DEE System. If your organization has a compelling need for that data which would justify procurement of the required items and loan to DISA, please contact us to discuss technical requirements and feasibility.

4.2.2. Vague or Undefined Search Criteria

When we get a search request, we design a query which is keyed into the DEE System. DISA cannot interpret requests—if the request isn't specific, we can't design a query and the search is, therefore, delayed.

DISA can't design queries for "including but not limited to" or "related to" keywords. The requester should either list all relevant keyword permutations or leave this part of the search blank. You'll get a larger results (more emails), but you are more likely to get the emails you need.

Likewise, we can't process a search for emails "on or about" a specific date, we need to know the date range.

4.3. Search versus Preservation versus Account Duplication

When DISA processes a request for DEE emails, by default we run a search, meaning we query the System for emails and attachments matching the requested search criteria and the System copies all matching emails into a .pst file set up specifically for the search. This .pst file contains exact copies of the query results, including headers. In the event the request is to preserve an account, we send the entire current contents of the account to the requester for them to preserve. Occasionally, a law enforcement organization will request that we create a special duplicate account, an account which duplicates the user's normal account but of which the user is unaware and which retains all activity in the account. Such duplicate accounts are only created at the properly documented and approved request of a law enforcement agency. It is not a substitute for a journalled account and will not be maintained indefinitely.

4.4. What Happens When You Request a Search

DISA Defense Enterprise Email (DEE) receives all incoming search results, logs the requests, confirms receipt, and sends them to DISA OGC for confirmation that the search documentation is sufficient. Once DISA OGC approves the search, then the DEE tech keys the queries into the System.

The DISA DEE tech will contact the requester if a search request can't be processed or if we encounter any problems. Most often rejections are caused by incomplete documentation or requests for searches of non-DEE target accounts.

Once the query is keyed into the System, the search will continue automatically until all emails matching the search criteria have been located and copied to a .pst file set up for the particular search. When the query completes, DISA DEE will upload the results (the .pst file) to one of two secured websites (classified or unclassified) and email the Requester with instructions on how to download the results. Once the data is available for download it is the requester's responsibility to download the data within a 14 day window. Otherwise, after the 14 days have expired, DISA DEE tech will delete the data from our local servers which means the requester will have to restart the process and face additional delays.

In order to ensure that the search results are not corrupted during the process, we apply a secure hash algorithm. The secure hash algorithm also provides chain of custody evidence—any changes to the data in the file will modify the value of the hash. This is proof to any court of inquiry that the data they are viewing was, indeed, the same data sent by DISA.

At no time during the process does DISA examine the emails returned in the search.

4.5. A Note about Encryption, Digital Signatures and Attachments

A digital signature or encryption acts like an envelope around the content of a message. If you add a digital signature *and* encrypt the message, you are wrapping the content in two envelopes.

An attachment is like a message inside the message. An attachment to a message with a digital signature is like an envelope inside an envelope.

DISA can search the outside of an envelope, meaning the header or the content of a message with just a digital signature, but we can't search the inside of an envelope. So we can't search the content of an attachment if the message itself is digitally signed. Likewise, we can't search the content of an encrypted message.

In order to ensure that you get the best results, especially in litigation discovery and investigations, we recommend you search for keywords only when they are likely to appear in the subject line of an email (which is the header).

5. Search Request Requirements

As discussed above, DEE emails belong to the DEE Mission Partner organization that provisions the account. DISA will make emails available upon request provided that we receive the appropriate documentation.

Please read through the relevant section below and be sure to include the required documentation with your search request. Failure to send the required documentation or incomplete documentation will delay the processing of your request.

Our intent is not to be uncooperative or bureaucratic, but to protect DEE emails and attachments from unauthorized or inappropriate access. When DISA performs a search, we do not look at or read the email results. Email search results may contain classified information, controlled but unclassified information, PII, or privileged information. We need to be sure that whomever we send the search results to is authorized to receive them.

Please remember:

The requesting organization is solely responsible for making release determinations and for ensuring compliance with all information handling laws, regulations, and policies.

5.1. FOIA Requests

Each DEE search request in response to a FOIA request must be sent by digitally signed email directly to DISA DEE LECI Support at:

disa.dscc.eis.mbx.cols-leci-requests@mail.mil

Please remember that DISA cannot estimate when a query will be completed, so FOIA Offices are encouraged to notify FOIA requesters of possible delays in fulfilling requests for emails. FOIA Offices should also be sure to include sufficient time to review the search results for release and/or redaction.

Each search request must include:

- ☑ DEE target accounts (email addresses), date ranges, and keywords or phrases.
- ☑ FOIA case number or other file designation.
- ☑ Confirmation by the FOIA Officer that the target accounts are provisioned by the organization or command making the DEE search request.
- ☑ Signature by the FOIA Officer (digital signature is acceptable) or explanation of why the FOIA Officer is not making the request.
- ☑ Government Point of Contact sending the request and receiving the results (can be the FOIA Officer; can't be contractor).
- ☑ If the target accounts belong to a legal counsel office (e.g., OGC attorneys), then the FOIA Officer must confirm that the legal counsel office has been notified of both the FOIA request and details of the search request.
- ☑ A signed statement from the FOIA Officer acknowledging that:

    1. The search results may contain information that is personal, privileged, or otherwise protected from release under a FOIA request.
    2. The requesting organization (DEE Mission Partner) agrees that it is solely responsible for withholding and redacting all documents produced by the search, including email subjects, texts, and attachments, and obtaining their own organization's legal approval for any release of information.

3. The requesting organization (DEE Mission Partner) agrees that it is solely responsible for contacting any other organization for clearance to release any information belonging to another organization which is produced by the search.

5.1.1. Helpful Hints for FOIA Requests

- The documents required above may be digitally signed emails, .pdf files, or Word files, or a scan of a "wet signature" document.
- Digital signatures must be valid and verifiable.
- DISA will ***not*** accept non-digital electronic signatures such as "//signed."
- Requests will not be processed until all required documentation is received.
- Remember that DISA will not interpret FOIA requests—see Section 4 for more information about search criteria.
- ***Your organization is responsible for making all release decisions, including redacting or withholding information.***

5.2. Investigation Requests

Each DEE search request pursuant to an investigation must be sent via digitally signed email directly to DISA DEE LECI Support at:

DISA DSCC EIS Mailbox Cols-LECI Requests
<disa.dscc.eis.mbx.cols-leci-requests@mail.mil>
or
DISA DSCC OPC Mailbox COLS LECI Requests
<disa.dscc.opc.mbx.cols-leci-requests@mail.smil.mil>

Please note that only a small team at DISA has access to these group email boxes. Throughout the DEE search process, we take every reasonable measure to ensure that investigation requests are accessed by the fewest DISA personnel necessary. If your investigation is of an outrageously sensitive nature, please contact either address above and ask to discuss alternate arrangements for submitting a request.

Each search request must include:

- ☑ DEE target accounts (email addresses), date ranges, and keywords or phrases, as applicable.
- ☑ Confirmation that the target accounts are provisioned by the same organization conducting the investigation or explanation of the authority of the investigating organization to request the search.
- ☑ Investigation number or other designation and a brief explanation of the nature of the investigation (e.g., counterintelligence, criminal, court martial, etc.). We don't need to know all the details, just the gist.
- ☑ Signature by the investigator making the request (digital signature is acceptable) and a Point of Contact to receive the results (usually the same person, but not a contractor).
- ☑ Appointment memo or other document signed by supervisor, Resident Agent-in-Charge, or other chain of command official stating that the search requester is assigned to the specific investigation and is authorized to request the DEE search and receive the results.
- ☑ Confirmation by the investigator or supervisor that legal counsel has approved the investigation or is advising the investigator through the course of the investigation and that the request is compliant with all relevant laws, regulations, and policies.

5.2.1. Helpful Hints for Investigation Requests

- The documents required above may be digitally signed emails, .pdf files, or Word files, or a scan of a "wet signature" document.

- Digital signatures must be valid and verifiable.

- DISA will ***not*** accept non-digital electronic signatures such as "//signed."

- Requests will not be processed until all required documentation is received, but DISA will cooperate to preserve as much evidence as possible. Please contact DISA DEE LECI Support if you have a very time-sensitive request.

- Generalized credentials or authorizations are not acceptable—we must have confirmation from your supervisor or chain of command that you are assigned to investigate the particular case.

- ***Your organization is responsible for complying with all relevant laws, regulations, and policies when collecting and using search results in your investigation. Contact your legal counsel for guidance.***

5.3. Litigation or Legal Requests

Each DEE search request pursuant to litigation, a court order, discovery request, etc., must be sent via digitally signed email directly to DISA DEE LECI Support at:

DISA DSCC EIS Mailbox Cols-LECI Requests
<disa.dscc.eis.mbx.cols-leci-requests@mail.mil>
or
DISA DSCC OPC Mailbox COLS LECI Requests
<disa.dscc.opc.mbx.cols-leci-requests@mail.smil.mil>

Please remember that DISA cannot estimate when a query will be completed, so litigators are encouraged to obtain necessary extensions or flexible deadlines.

Each search request must include:

- ☑ DEE target accounts (email addresses), date ranges, and keywords or phrases, as applicable.
- ☑ Confirmation that the target accounts are provisioned by the same organization making the search request or explanation of the authority of the litigator to request the search.
- ☑ The first page and the signature page from the court order, discovery request, court martial charge, or other relevant filing related to the search request.
- ☑ Signature by the litigator or attorney making the request (digital signature is acceptable) and a Point of Contact to receive the results (usually the same person, but not a contractor).
- ☑ Statement by the litigator or legal counsel that the search request is pursuant to current litigation or is being made in anticipation of litigation.
- ☑ Confirmation by the litigator or legal counsel that the request is compliant with all relevant laws, regulations, and policies.
- ☑ Confirmation by the litigator or legal counsel that the requesting organization is solely responsible for any and all release decisions when using the emails as evidence or in response to a discovery request or court order.

5.3.1. Helpful Hints for Investigation Requests

- The documents required above may be digitally signed emails, .pdf files, or Word files, or a scan of a "wet signature" document.
- Digital signatures must be valid and verifiable.
- DISA will ***not*** accept non-digital electronic signatures such as "//signed."
- Requests will not be processed until all required documentation is received.
- DISA cannot search local drives, so litigators may need to contact individual users or network administrators for emails stored locally.
- ***Your organization is responsible for complying with all relevant laws, regulations, and policies, including determining whether emails and attachments are releasable under court orders or discovery requests.***

5.4. Third-Party Access Requests

DISA gets periodic requests for access to an individual user's emails because the user has unexpectedly left the Department of Defense, passed away, or is out for an extended period of time. Upon request, DISA will start an Out-of-Office message for the user directing senders to another user or another point of contact.

If a supervisor of an employee needs access to a subordinate's emails, they will need to provide a memorandum from the first O-6 or GS-15 in their chain of command explaining the reason access is needed. For example: "I am CAPT James T. Kirk. LCDR Montgomery Scott, my Chief Engineer, was tragically killed when his shuttle craft crashed into a Dyson Sphere. There is vital engine data stored in his e-mail account which must be processed or the dilithium crystals will explode."

For these searches, the request must be sent by digitally signed email directly to DISA DEE LECI Support at:

DISA DSCC EIS Mailbox Cols-LECI Requests
<disa.dscc.eis.mbx.cols-leci-requests@mail.mil>
or
DISA DSCC OPC Mailbox COLS LECI Requests
<disa.dscc.opc.mbx.cols-leci-requests@mail.smil.mil>

Each search request must include:

- ☑ DEE target account (email address), date ranges, and keywords or phrases.
- ☑ Description of justification for search (e.g., reason why the employee's e-mail is inaccessible).
- ☑ Confirmation by the requester that the target accounts are provisioned by the organization or command making the DEE search request.
- ☑ Government Point of Contact sending the request (can't be contractor).
- ☑ Designation of recipient who will receive the results.

5.4.1. Helpful Hints for Third-Party Access Requests

- The documents required above may be digitally signed emails, .pdf files, or Word files, or a scan of a "wet signature" document.
- Digital signatures must be valid and verifiable.
- DISA will ***not*** accept non-digital electronic signatures such as "//signed."
- Requests will not be processed until all required documentation is received.

5.5. Special Requests and NARA Archiving

DISA does not send DEE emails to NARA for archiving, so DEE Mission Partners should request a search for any emails that should be archived. In addition, DEE Mission Partners may need to request a search that does not fall into the categories described in Sections 5.1-5.4. For these searches, the request must be sent by digitally signed email directly to DISA DEE LECI Support at:

DISA DSCC EIS Mailbox Cols-LECI Requests
<disa.dscc.eis.mbx.cols-leci-requests@mail.mil>
or
DISA DSCC OPC Mailbox COLS LECI Requests
<disa.dscc.opc.mbx.cols-leci-requests@mail.smil.mil>

Each search request must include:

- ☑ DEE target accounts (email addresses), date ranges, and keywords or phrases.
- ☑ Description of purpose of search (e.g., NARA archive).
- ☑ Confirmation by the requester that the target accounts are provisioned by the organization or command making the DEE search request.
- ☑ Government Point of Contact sending the request and receiving the results (can be the FOIA Officer; can't be contractor).
- ☑ If the target accounts belong to a legal counsel office (e.g., OGC attorneys), then the requester must confirm that the legal counsel office has been notified of the details of the search request.
- ☑ If the search results may be released or transferred to another DoD organization or outside DoD, a signed statement from the Requester's ***chief legal counsel*** acknowledging that:

    1. The search results may contain information that is personal, privileged, or otherwise protected from release to the public or outside DoD.
    2. The requesting organization (DEE Mission Partner) agrees that it is solely responsible for protecting, withholding and/or redacting all documents produced by the search, including email subjects, texts, and attachments.

3. The requesting organization (DEE Mission Partner) agrees that it is solely responsible for contacting any other organization for clearance to release any information belonging to another organization which is produced by the search.

5.5.1. Helpful Hints for Special Requests

- The documents required above may be digitally signed emails, .pdf files, or Word files, or a scan of a "wet signature" document.
- Digital signatures must be valid and verifiable.
- DISA will ***not*** accept non-digital electronic signatures such as "//signed."
-
- Requests will not be processed until all required documentation is received.
- Remember that DISA will not interpret requests—see Section 4 for more information about search criteria.

- ***Your organization is responsible for protecting the search results and making all release decisions, including redacting or withholding information.***

6. Where to Get Help or More Information

If you have questions about submitting a DEE search request, please contact:

DISA DSCC EIS Mailbox Cols-LECI Requests
<disa.dscc.eis.mbx.cols-leci-requests@mail.mil>
or
DISA DSCC OPC Mailbox COLS LECI Requests
<disa.dscc.opc.mbx.cols-leci-requests@mail.smil.mil>

This document has been prepared by the
DISA Office of General Counsel and is current as of October 11, 2016.