



# Joint Cyber Intelligence Tool Suite (JCITS) Malware Intelligence Triage Tool (JMITT)



## (U) Joint Cyber Intelligence Tool Suite Malware Intelligence Triage Tool (JMITT) email submission procedures for the Cleared Contractor

(U) Defense Counterintelligence and Security Agency (DCSA) utilizes Georgia Tech Research Institute's (GTRI) Apiary product to analyze suspected malicious files only (not URLs). DCSA procured its own instance of Apiary from GTRI, newly named JMITT that is available for use by the cleared contractor. The improved validation and verification process, through the use of the Joint Intelligence Tool Suite (JCITS) will help better prioritize incoming malicious files. While the tool is beneficial to the CC, DCSA Counterintelligence (CI) Special Agent, and DCSA CI Cyber Team, it is not all encompassing and should not be considered absolute.

(U) Apiary automatically ingests, processes, and analyzes suspected malware or suspicious attachments, making the association **RESULTS IMMEDIATELY AVAILABLE TO THE CLEARED CONTRACTOR**, the DCSA CI Special Agent, and DCSA CI Cyber Team. The system utilizes multiple methods of correlation to provide links between malware samples that may otherwise remain disconnected and invisible to DCSA Cyber analysts.

(U) Cleared contractors can submit suspected malicious email attachments directly to JMITT via email.

**Note:** Prior to submitting samples to Apiary please coordinate with your Facility Security Officer (FSO) to review for potential classified or controlled technology information, recruitment attempts, illegal acquisition or elicitation.

## (U) Procedures for sending suspected and/or unknown potentially malicious attachments to JMITT:

(U) Attach suspected email message/file(s) to a new email message using the following procedures:

1. Create a New Email message.
2. To Line: [submit@dss.apiary.gtri.org](mailto:submit@dss.apiary.gtri.org)
3. Subject Line: **ABC12** *\*\*Subject Line must include a valid CAGE Code to be processed.*
4. Copy the suspected malicious email message with attached file(s) to the new email message. Procedures may vary depending on which email application you use.
5. Send the email message unencrypted.

# Joint Cyber Intelligence Tool Suite (JCITS) Malware Intelligence Triage Tool (JMITT)



(U) Once the suspected malicious attachment is sent to JMITT, the cleared contractor and local DCSA CI Special Agent will receive an automatic email reply from JMITT indicating if the submission was either successfully ingested or rejected. If the submission was rejected, forward the rejection email to the local DCSA CI Special Agent, with a courtesy copy to the DCSA CI Cyber Division at [dcsa.quantico.dcsa-hq.mbx.dss-cyberci@mail.mil](mailto:dcsa.quantico.dcsa-hq.mbx.dss-cyberci@mail.mil). DCSA CI Cyber Team will work with the CI Special Agent and cleared contractor to ensure the submission issue is resolved.

## (U) File Types

(U) JMITT can ingest and analyze the following file types (available analyses varies based on the file type):

*Archive Files:* gzip, pkzip, rar, arj, cab, zip, ace, msa, generic archive, android, jar

*Document Files:* office, cdf, pdf, rtf

*Executables:* coff, elf, mach-o, ms-dos, pe, java

*Scripts:* perl script, python script, bash script, posix script, /bin/sh script, ruby script, generic script

*Libraries:* dll

*Media:* flash, html, image, mpeg, riff

