MITS Security Request Process

The AD-1143 Corporate Systems Access Request Form should be completed to request access to MITS and the respective MITS modules. The AD-1143 has now been updated to include MITS specific details for each of the MITS modules. The form now includes MITS specific information in block 32 which should be completed by the requester to include the required role, programs, and agencies. Specific MITS completion instructions are included in the instructions section at the end of the form. If multiple roles are to be requested for a single module such as PMA, a separate AD-1143 should be completed for each role.

Once completed, the form will have to be signed and approved per the AD-1143 instructions by the user, the user's manager, and the agency security administrator. If multiple agencies are requested, the agency security administrator for each agency noted will need to sign the AD-1143.

Once the form is completed including appropriate signatures, it should be scanned and forwarded to the MITS Security Administrator at mits.security@usda.gov. If the requester doesn't have access to a scanner, the Agency Security Officer or the MITS Help Desk can be asked to scan and forward the request. Anyone (requester, manager, Security Administrator, etc) can forward the AD-1143 to the MITS Security Administrator.

The MITS Application Security Administrator at NITC will monitor mits.security@usda.gov for incoming AD-1143 submissions. The MITS Application Security Administration Team at NITC will provide the requested access after verifying that the form is correctly completed. If the form is not completed correctly including required signatures, it will be returned. The MITS Security Administrator will notify the user and Agency Security Administrator once the requested access has been established. The notification to the user will include the MITS address https://MITS.OCFO.USDA.GOV where the user can access MITS.

The MITS Application Security Administrator will electronically file all successfully completed AD-1143 security requests. This copy is not the original or the official copy of the form, but will serve as a record of the AD-1143's received and processed.

Agency Security Administrators can contact the MITS Security Administration Team at NITC (816-823-2859) to address any issues relative to the processing of individual requests.

A copy of the AD-1143 Corporate Systems Access Request Form can be obtained from the following website:

http://www.ocio.usda.gov/forms/ocio_forms.html

The following is a list of the MITS security roles and definitions for each of the MITS modules:

PMA Roles

Agency User: Agency Users can enter data for self-evaluations such as scores, evidence data, status, and actions.

Approving Official: Approving Officials can review and overwrite the scorecard information for their agencies prior to submitting the scorecards to Initiative Owners. Agency Users cannot be Approving Officials.

Initiative Owner: (Department) Initiative Owners will have access to all agencies' scorecards under their initiatives. They can also overwrite scores, evidence, files, deliverables status, and comments submitted by agencies. The Initiative Owner may scan import, add, edit, and delete criteria/metrics/check lists within their initiatives.

Executive Officer: Executive Officers include the Deputy Secretary, senior management officials, and sub-cabinet officials. Executive Officers can retrieve the final scorecard reports, view trend analysis, and generate custom reports from the system.

PMA Coordinator: The PMA Coordinator can review scorecards, generate final summary reports, and generate custom reports. The PMA Coordinator can edit and change all data.

PART Roles

Agency User: Agency Users have read access for all USDA PARTs and edit access for select PARTs. Agency Users do the majority of the input, but do not have the ability to submit materials.

Approving Official: Approving Officials have read access for all USDA PARTs and edit access for all agency PARTs. Approving Officials may edit material and have the ability to submit PARTs, milestones and performance measures to the Mission Area and OBPA.

Mission Area Coordinator: Mission Area Coordinators have read access for all USDA PARTs. They can edit all Mission Area PARTs, request agency edits, or submit PARTs to OBPA.

Executive Officer: Executive Officers include senior management officials. Executive Officers can retrieve reports, view trend analysis, and generate custom reports from the system.

OBPA Officer: The OBPA Officer requires 'viewing only' access. The OBPA Officer must be an OBPA employee. They have read access for all USDA PARTs and edit access for select PARTs. They can request agency edits and submit PARTs to OMB.

Budget Tracking Roles

Agency Users: Agency Users can enter data for the budget templates for their agency or Mission Area only.

A**pproving Officials**: Approving Officials (Agency Budget Officers) can review and overwrite the budget information for their agencies or mission areas prior to submitting the budget templates to the OBPA or back to agency users. This role is for agency or Mission areas only.

Executive Officers: Executive Officers include senior management and can generate all tracking reports from the system. Executive Officers do not have write access; they can only view reports and data. This would include agency and mission area managers.

OBPA Coordinators: OBPA Coordinators can edit and change all data for all agencies EXCEPT archived data. OBPA Coordinators are the final approving authority for budget template submissions. OBPA Coordinators must be OBPA employees.

Audit Tracking Roles

Agency Users: Agency users include the audit liaison officials and their staff. Agency users can review all data within their given agency. Additionally, they can only edit/create corrective action plan and status information for their agency's audits.

Executive Officers and OIG Auditors: Executive Officers include the senior management officials within the OCFO. Executive Officers and OIG Auditors can view all agencies data and generate standard and custom reports from the system. Executive Officers and OIG Auditors cannot modify, add or delete data.

Audit Follow-up Coordinator: Audit Follow-up Coordinators consist of management staff within the OCFO – Planning and Accountability Division. Audit Follow-up Coordinators can review, manage, create, edit, and delete (limited delete) all data. This is the highest level of authority in the Audit Tracking Module.