THE INDIAN HEALTH SERVICE

RPMS Direct Messaging (Secure Messaging)

Presented by Marilyn Freeman

California Area HIM Consultant

Superior Health Information Management
Now and for the Future

DRAFT

RPMS Direct Messaging Team

- Glenn Janzen, Chief Enterprise Architect - IHS
- Chris Lamer, Clinical Informatics Consultant - IHS
- Meghna Patel, Business Analyst - DNC
- Duane Rosznyai, Application System Analyst – DNC

DRAFT

Key Terms

- **RPMS DIRECT:** A standard based, secure, point-to-point, web-based messaging system. It is intended for the exchange of patients' health information between healthcare Providers, such as Physicians, Nurse Practitioners, Physician Assistance, Medical Assistance, and other Healthcare providers who regularly transmit and/or receive Protected Health Information/Personally Identifiable Information (PHI/PII).
- **Certificate Authority:** An authority trusted by the IHS Health Information Service Provider (HISP) for issuance and management of certificates.
- **Registration Authority:** An authority trusted by the IHS HISP that works in collaboration with the IHS trusted CA to collect and verify information of the certificate subjects such as RPMS DIRECT Administrators and will evaluate to either approve or reject subscriber certificate management transactions, including certificate renewal, re-key, and revocation requests.
- **Domain Name:** A fully qualified domain name that identified the organization that assigns the health endpoint names and is dedicated solely to the purpose of health information exchange. Example: facilityname.directihs.net.

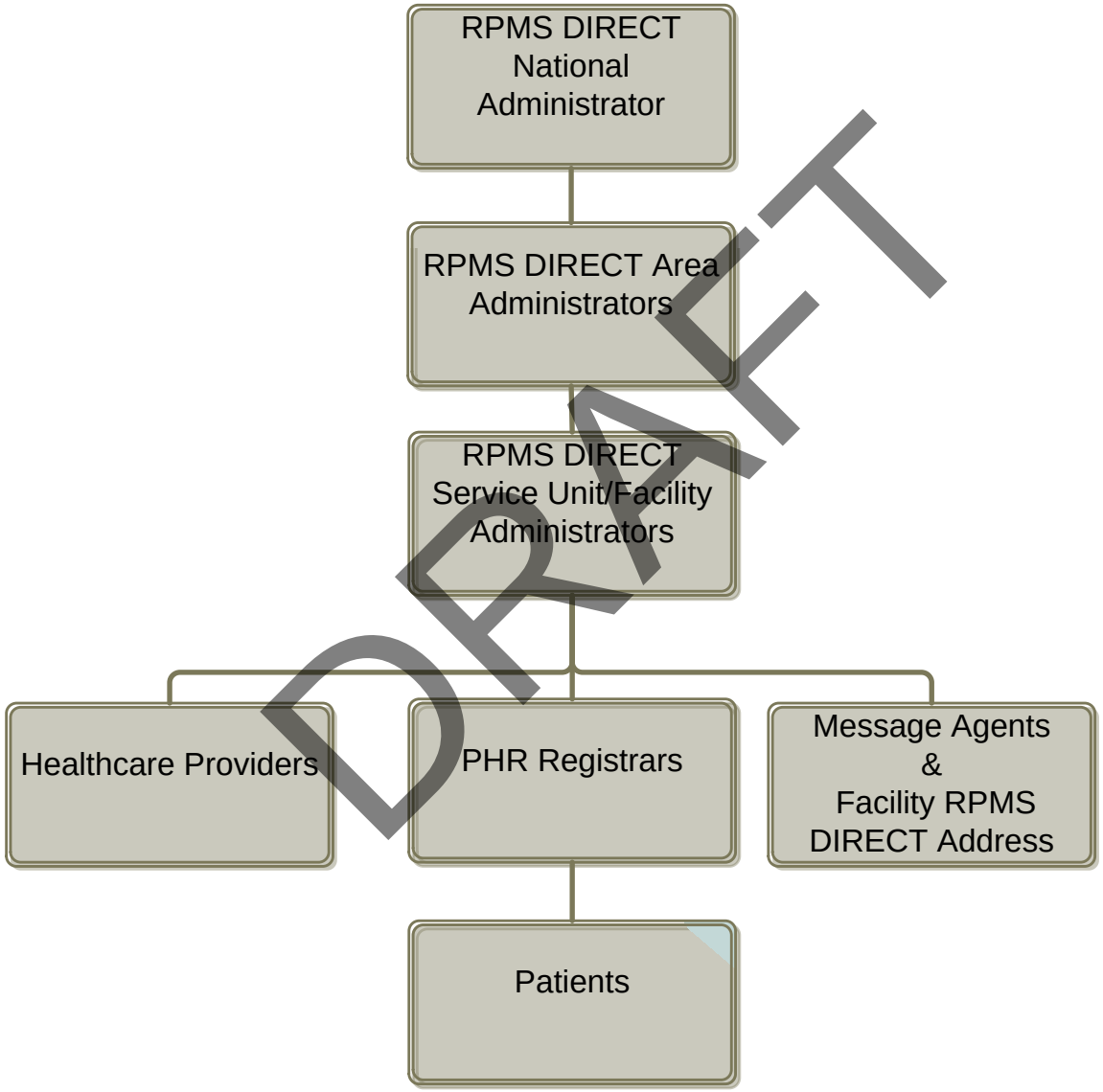
DRAFT

Key Terms

- **Message Agent:** An individual assigned to receive secure messages on behalf of healthcare provider(s). Messaging Agent's responsibility is assigned usually to the same person assigned to answer the phone in the clinic. Similar to the calls, Message Agent will get the messages, respond, and/or distribute them to the appropriate party.
- **Trusted Agent:** The Trusted Agent is an individual appointed on behalf of the Registration Authority to complete an in-person identity verification of the RPMS DIRECT users. The RPMS DIRECT Administrators will serve as a Trusted Agent.
- **SU/FA:** Service Unit/Facility Administrator
- **CSR:** Certificate Signing Request
- **DCV:** Domain Control Validation

DRAFT

Role Hierarchy



DRAFT

Area Administrator Responsibilities

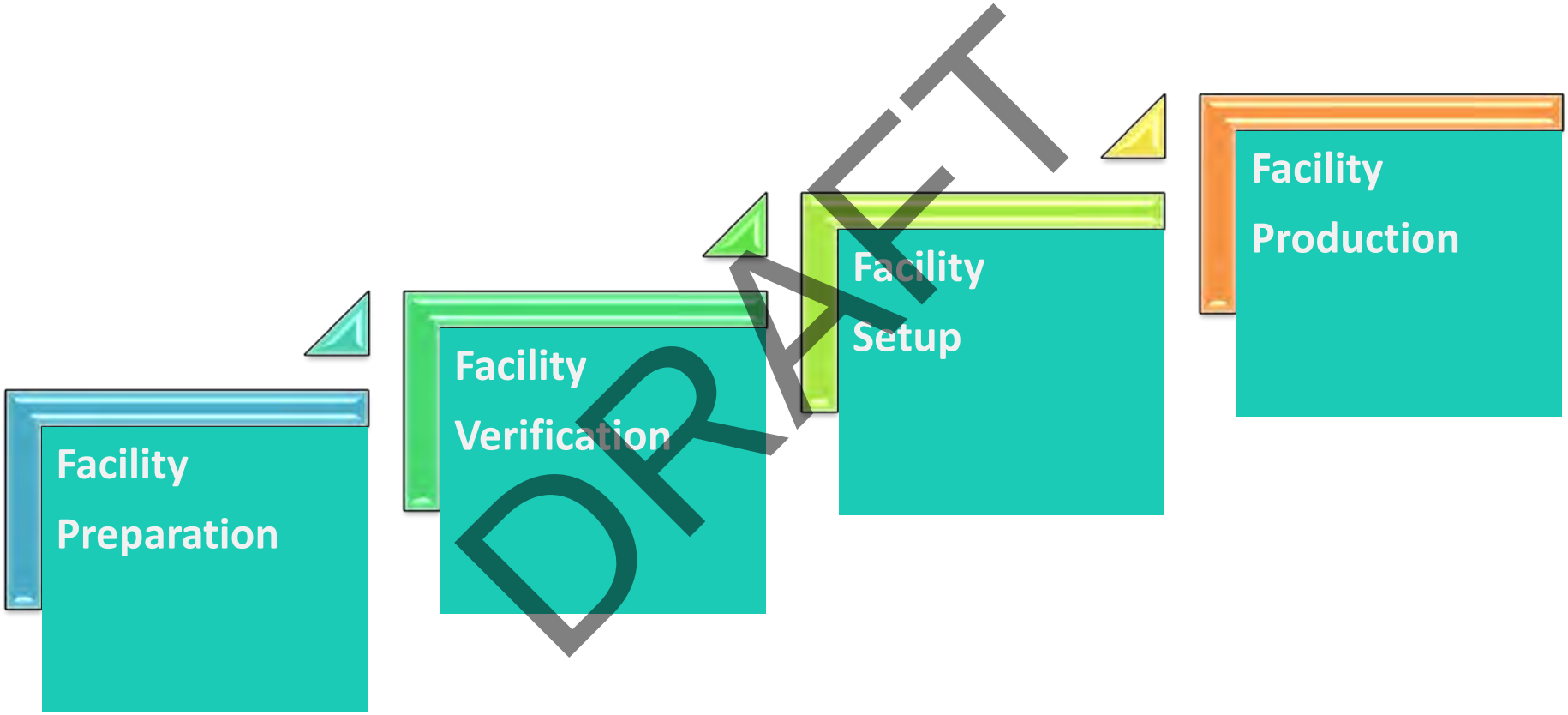
- Onboarding support to Service Unit/Facility (SU/F)
  - Prepare SU/F for deployment
  - Verify SU/F's readiness for deployment
  - Setup SU/F for deployment
    - Setup SU/F in the Certificate Portal
    - Order organization certificate
    - Setup SU/F in the RPMS DIRECT Administrative Application
  - Complete/validate deployment/production

- On-going support to SU/F
  - Tier 1 and 2 support to SU/FA
  - Tier 2 and 3 Support to SU/F
  - Access Management: ITAC System and Help Desk Tickets

- Regular Audits

DRAFT

Deployment Phases



Facility Deployment: Phase 1 & 2

Preparation

- **Establish Local RPMS DIRECT Team**
  - Service Unit/Facility Administrator (SU/FA)
  - Message Agents
  - Facility RPMS DIRECT Address Designee
  - PHR Registrars
  - Clinical Application Coordinator (CAC)

- **Complete RPMS DIRECT Pre-Requisite Task**
  - Agreements (i.e. ISA, BAA, and EUA; Multi-Purpose Agreement)
  - Trainings for Local Team
  - Policies and Procedure development and incorporation
  - Contingency plan
  - Outreach

Verification

- **Complete Readiness Assessment Form**

- **Verify Readiness Assessment Form and Related Tasks**

DRAFT

Facility Deployment: Phase 3 & 4

- **Setup HCO and SU/FA in the Portal**
- **ID Vetting of SU/FA**
- **Order and Map Facility Domain Certificate**
- **Add RPMS DIRECT Messaging Menu in the EHR**
- **Setup Facility Domain and SU/FA in the hMail Application**

- **Setup Local RPMS DIRECT Team**
- **Verification and Testing**
- **Onboard Users**
  - Registration
  - Training
  - Setup
- **Additional Trainings and Support**
- **Ready to Send and Receive Messages**

- **Ready to Send and Receive Secure Messages**

DRAFT

Applications

- **Certificate Authority Portal**
  - Order and approve Certificates and manage representatives and Trusted Agents for both Area and Site.
- **hMail Administrative Application**
  - Complete implementation, perform audits, and manage domain, administrator, and user access.
- **RPMS DIRECT Messaging Webmail**
  - Connects Healthcare providers and other healthcare professional to the RPMS DIRECT Messaging via RPMS-EHR.

DRAFT

Certificate Authority Portal

Access limited to:

- National Administrators
- Area Administrators

Functions:

- Set-up HCO
- Order
  - Organization certificates
  - Address certificates
- Manage
  - Contacts
  - Users
  - Domains
  - Certificates: Issue new, reissue, and revoke

DRAFT

Portal Role & Access

Defined Roles and Access within the CA Portal

	Role	Access
National Administrator	ISSO, Trusted Agent	Admin
Area Administrator	Trusted Agent	Operator
Service Unit/Facility Administrator	Representative, Trusted Agent	No Access

DRAFT

Area Administrator Setup

1. ITAC System: RPMS DIRECT Area Admin
2. Complete DigiCert Declaration Form

From: DigiCert <admin@digicert.com>
To: Patel, Meghna (IHS/HQ) [C]
Cc:
Subject: Please complete the required identity form for Indian Health Service

digicert

Hello Meghna Patel,

Indian Health Service has requested a certificate for use with Directed Exchange messaging they manage for your organization. Before DigiCert can issue this certificate, DirectTrust requires that your identity be verified.

Please visit the link below to ensure that your personal information is correct and to give Indian Health Service permission to manage this certificate on your behalf.

https://www.digicert.com/direct/contact-update.php?token=

If you have any questions please contact DigiCert Support or your account manager at Indian Health Service.

To learn more about DigiCert's role in Directed Exchange please visit this link.

www.digicert.com/direct-project/what-is-the-direct-project.htm

To learn more about DirectTrust please visit this link.

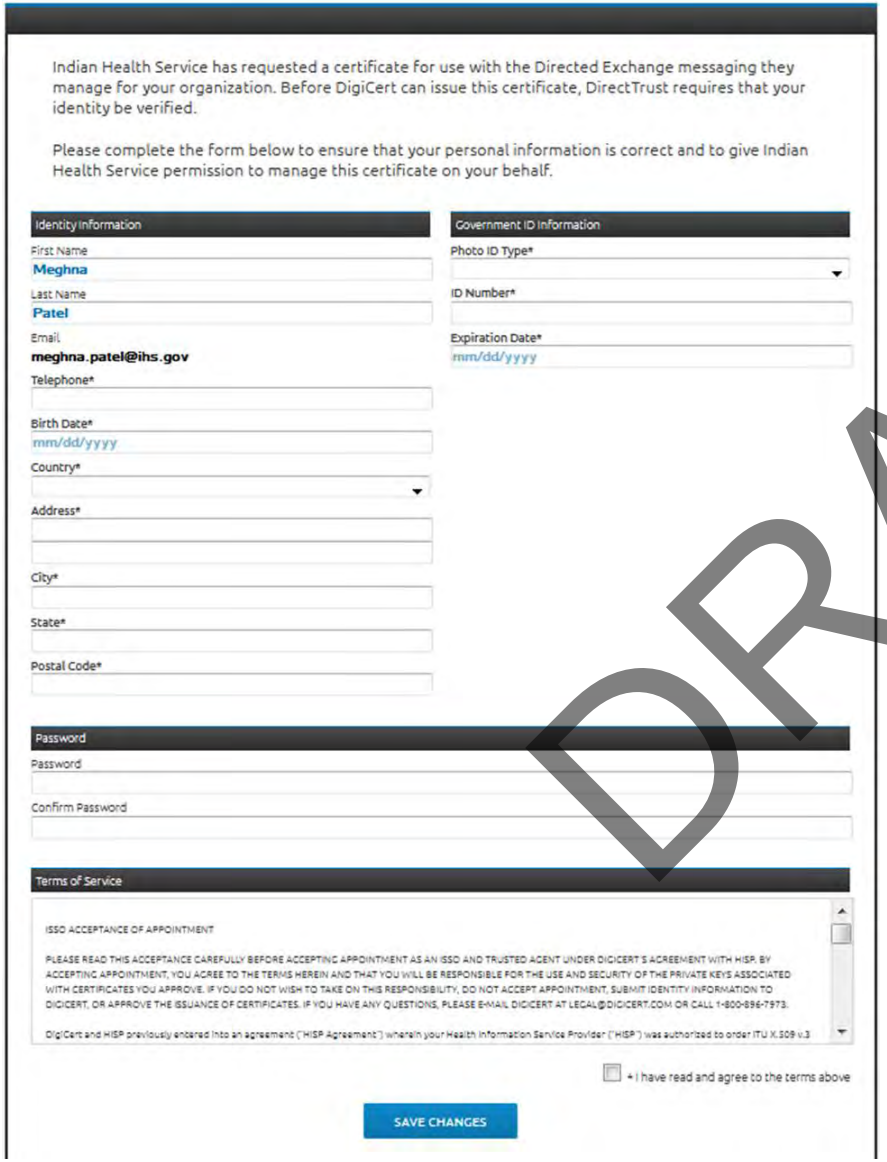
www.directtrust.org/directtrust-101/

Thank you,

DigiCert Support
Online: www.digicert.com
Support: support@digicert.com
Phone: 1-801-877-2100
Toll Free: 1-800-896-7973 (US & Canada)
Fax: 1-866-842-0223 (Toll Free - US & Canada)

DRAFT

AA Declaration Form



Indian Health Service has requested a certificate for use with the Directed Exchange messaging they manage for your organization. Before DigiCert can issue this certificate, DirectTrust requires that your identity be verified.

Please complete the form below to ensure that your personal information is correct and to give Indian Health Service permission to manage this certificate on your behalf.

Identity Information

First Name: Meghna
Last Name: Patel
Email: meghna.patel@ihs.gov
Telephone*
Birth Date*: mm/dd/yyyy
Country*
Address*
City*
State*
Postal Code*

Government ID Information

Photo ID Type*
ID Number*
Expiration Date*: mm/dd/yyyy

Password

Password
Confirm Password

Terms of Service

ISSO ACCEPTANCE OF APPOINTMENT

PLEASE READ THIS ACCEPTANCE CAREFULLY BEFORE ACCEPTING APPOINTMENT AS AN ISSO AND TRUSTED AGENT UNDER DIGICERT'S AGREEMENT WITH HISP. BY ACCEPTING APPOINTMENT, YOU AGREE TO THE TERMS HEREIN AND THAT YOU WILL BE RESPONSIBLE FOR THE USE AND SECURITY OF THE PRIVATE KEYS ASSOCIATED WITH CERTIFICATES YOU APPROVE. IF YOU DO NOT WISH TO TAKE ON THIS RESPONSIBILITY, DO NOT ACCEPT APPOINTMENT, SUBMIT IDENTITY INFORMATION TO DIGICERT, OR APPROVE THE ISSUANCE OF CERTIFICATES. IF YOU HAVE ANY QUESTIONS, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-896-7973.

DigiCert and HISP previously entered into an agreement ("HISP Agreement") wherein your Health Information Service Provider ("HISP") was authorized to order ITU X.509 v.3

* I have read and agree to the terms above

SAVE CHANGES

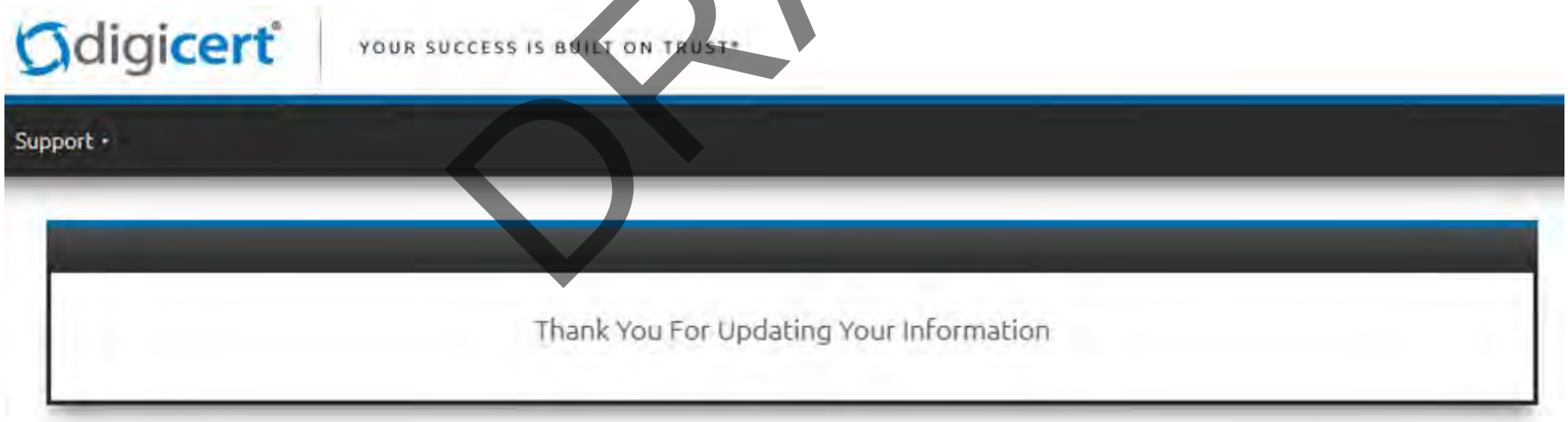
DRAFT

- **Email:** Enter work email address. This will be used to request more information for you and any future communication in regards to your account and domain. This email address will become your CA portal User ID.
- **Address:** Your home address as this will be used to identify your identity.
- **Government ID Information:** Select PIV Card from the dropdown.
- **Password:** Password length must be 8 or longer, contain a capital letter and either a number or special character.
- **Terms of service:** Read and accept DigiCert Terms of service by checking the checkbox
- **Save Changes**

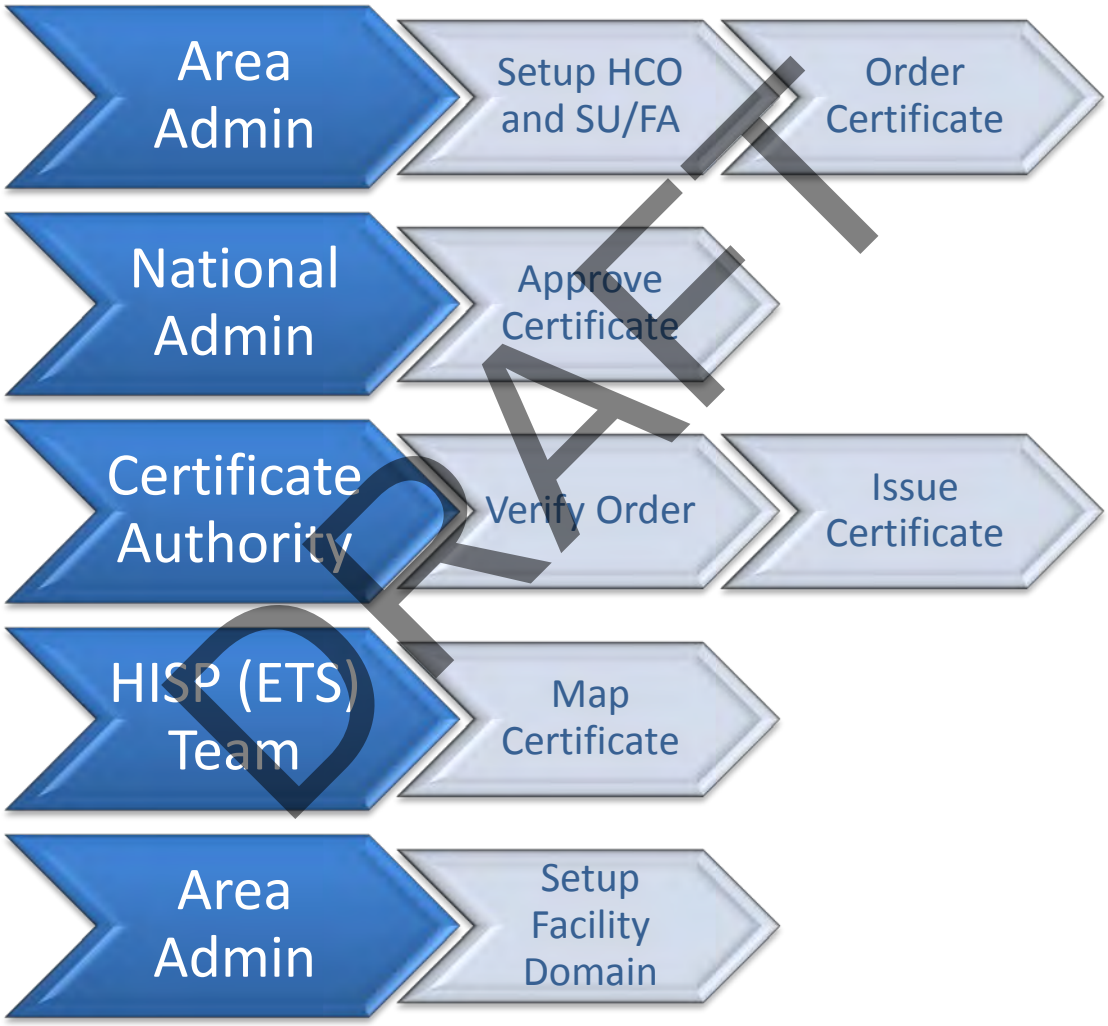
Area Administrator

- Upon successful completion of the form, all the information/form is submitted to DigiCert for your ID proofing
- Setup complete for Area Administrator
- Upon completion ID proofing you are now ready to:
  - Setup HCO
  - Request org. certificates

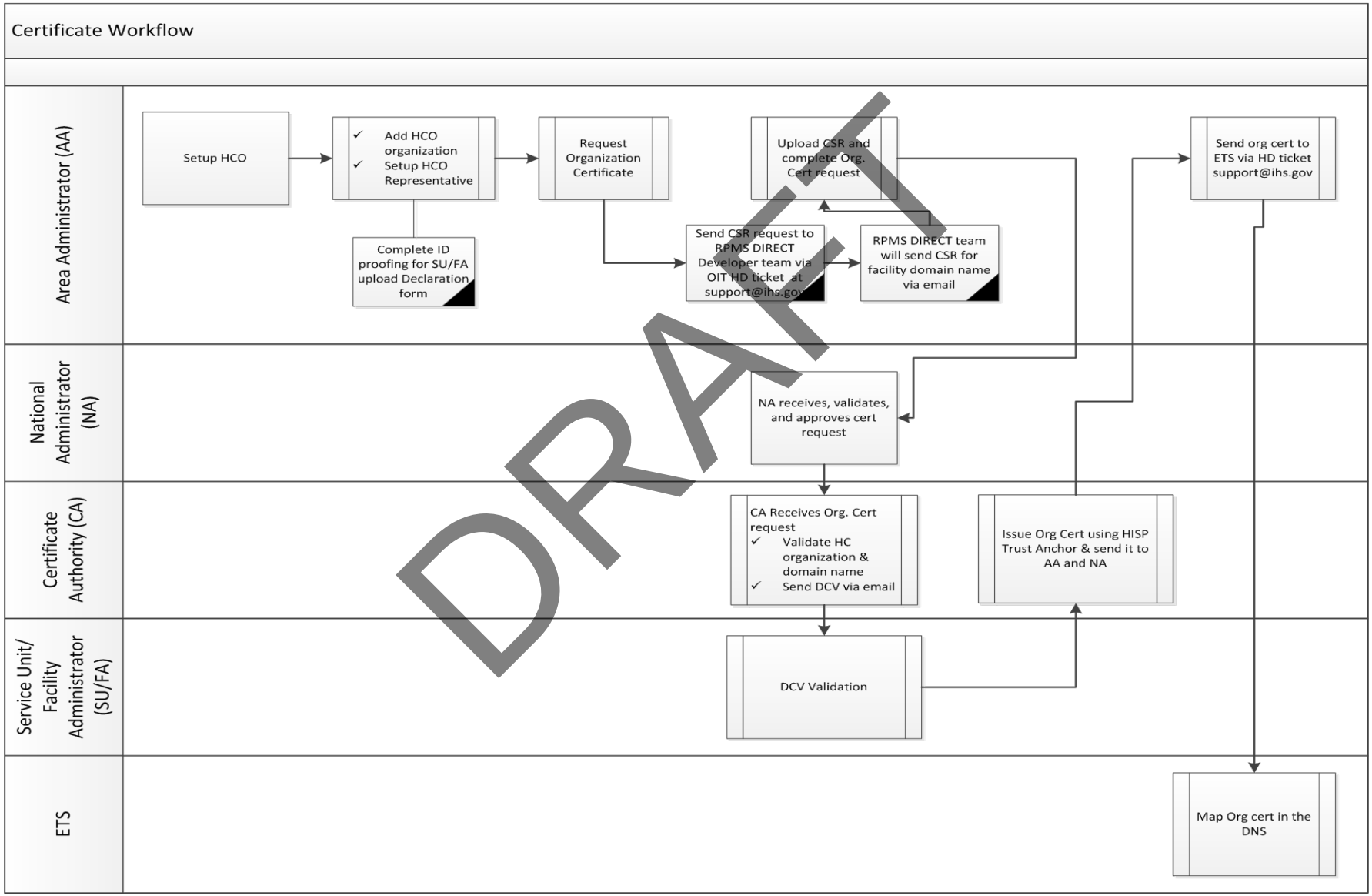
DRAFT



Simplified Certificate Workflow

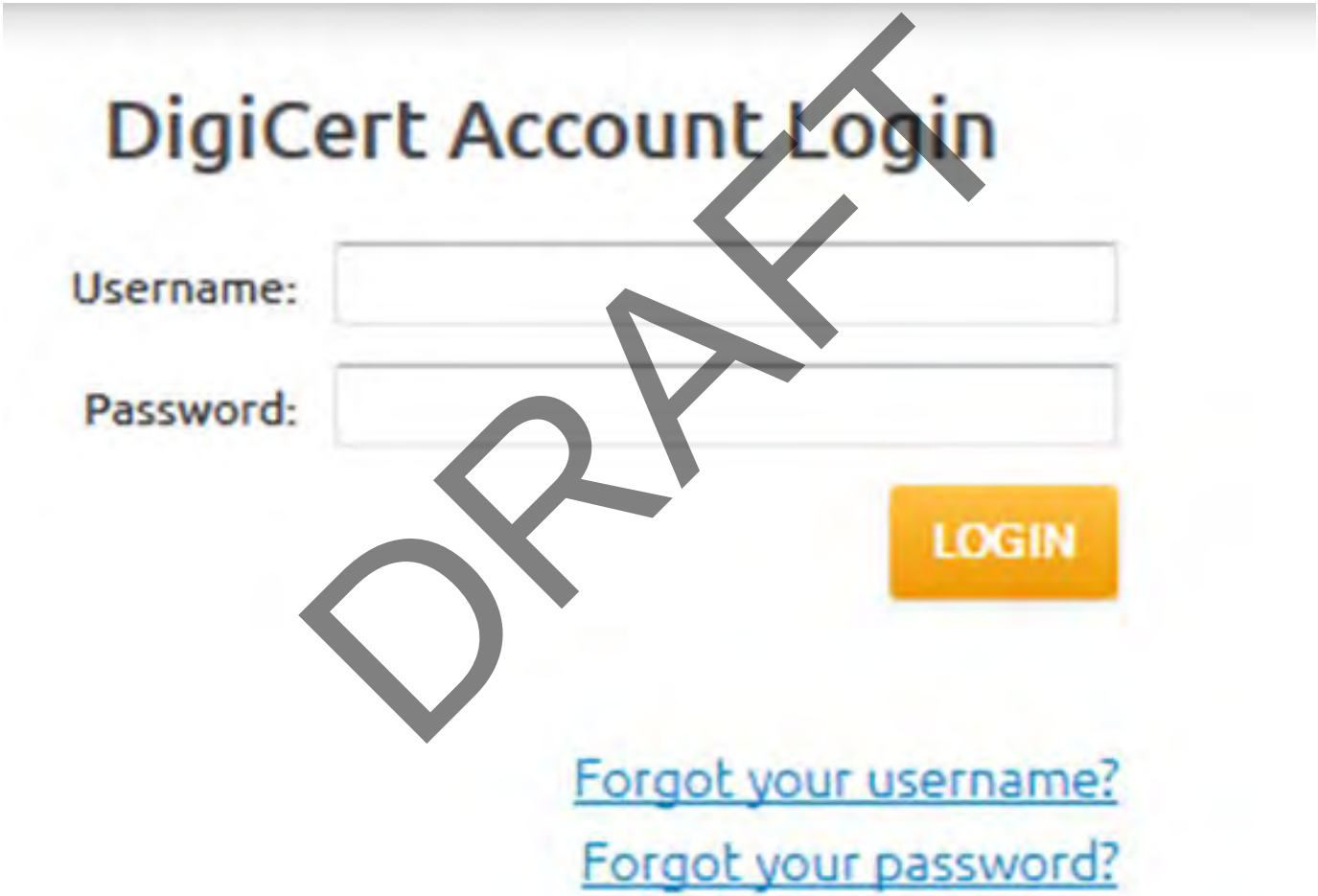


Certificate Workflow in Detail



Certificate Authority Portal

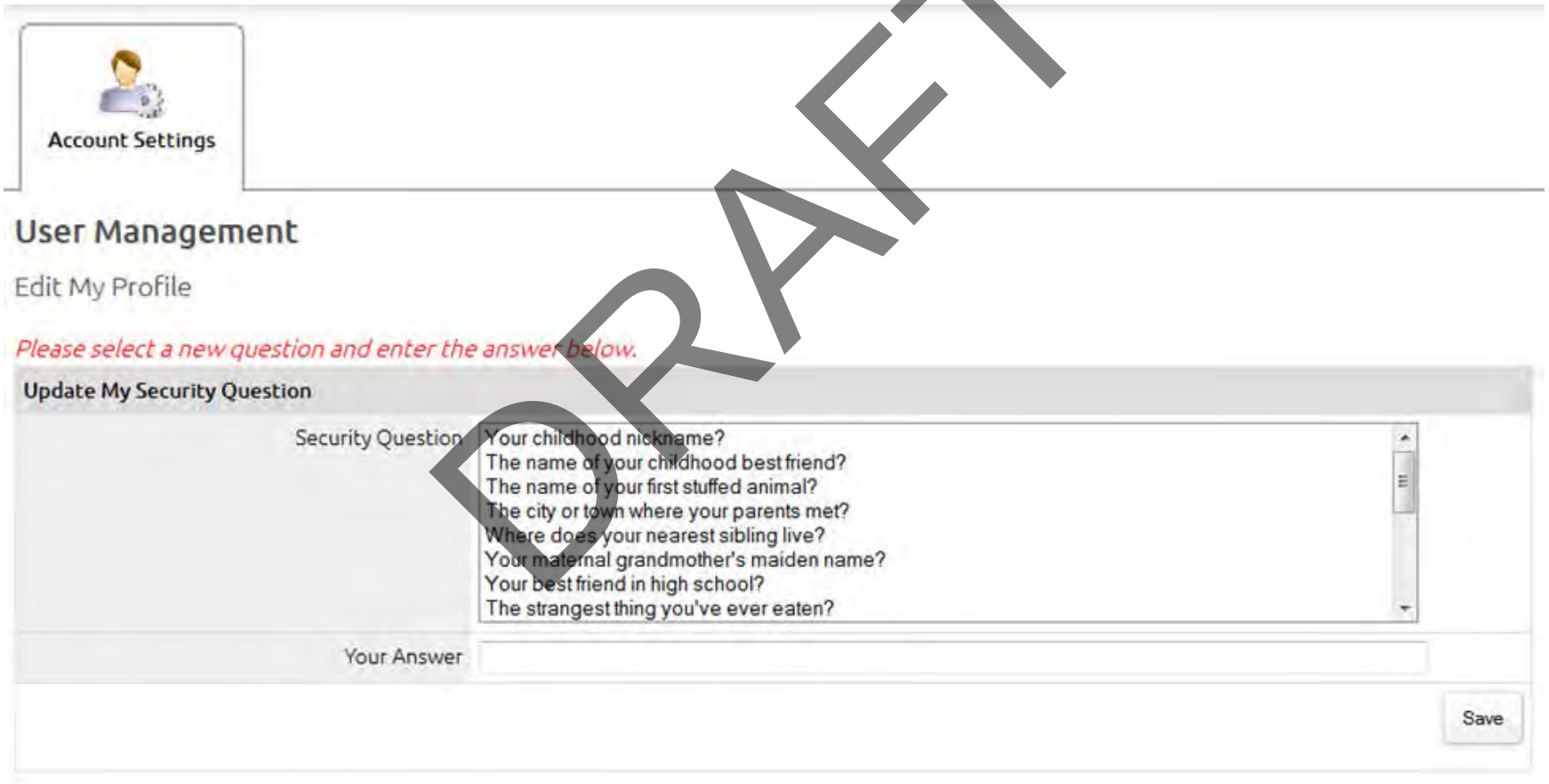
https://www.digicert.com/account/login.php



DRAFT

Certificate Authority Portal

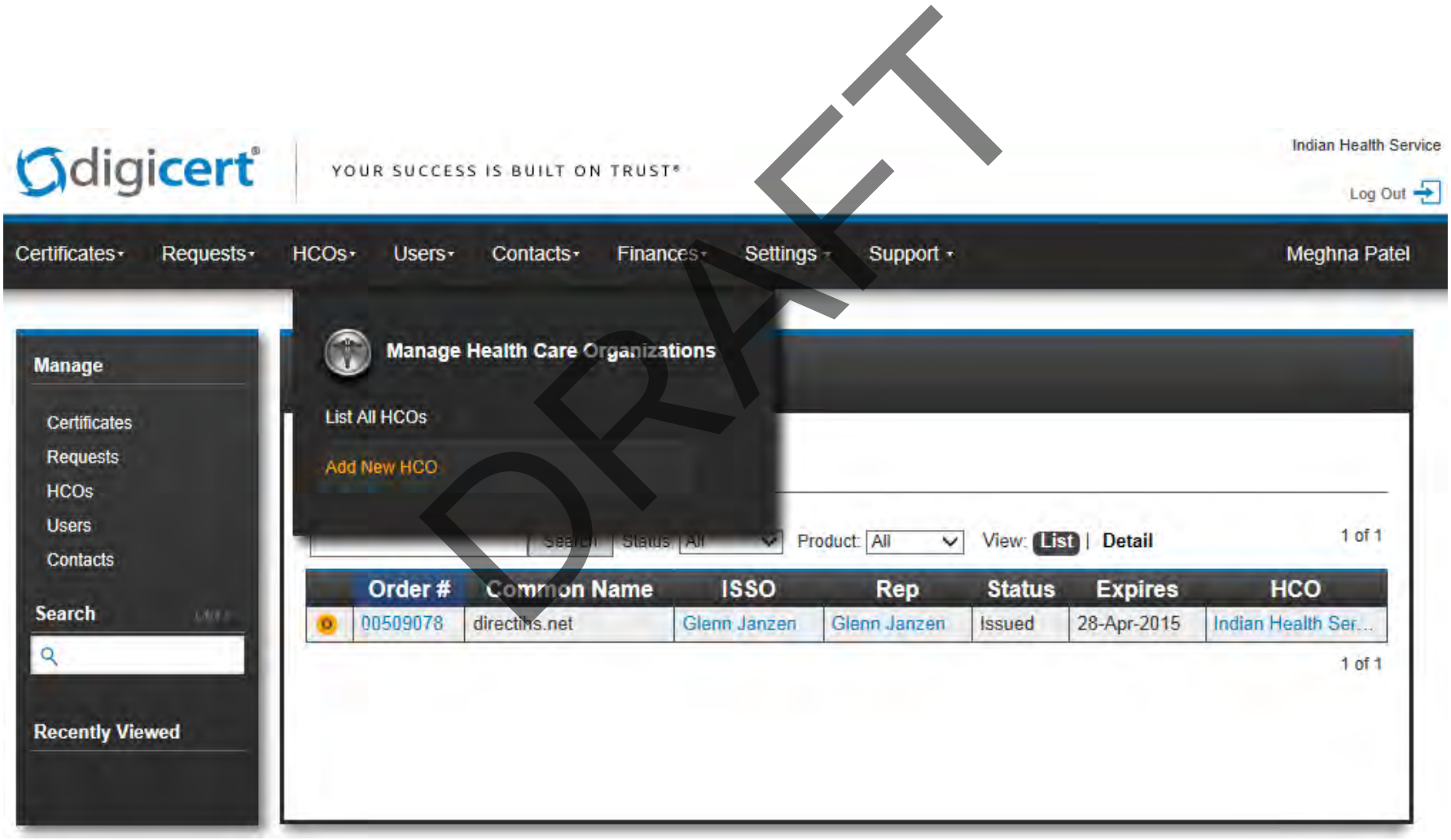
First time user will be required to set security question and answer



DRAFT

Add HCO

1. HCO→ Add New HCO



DRAFT

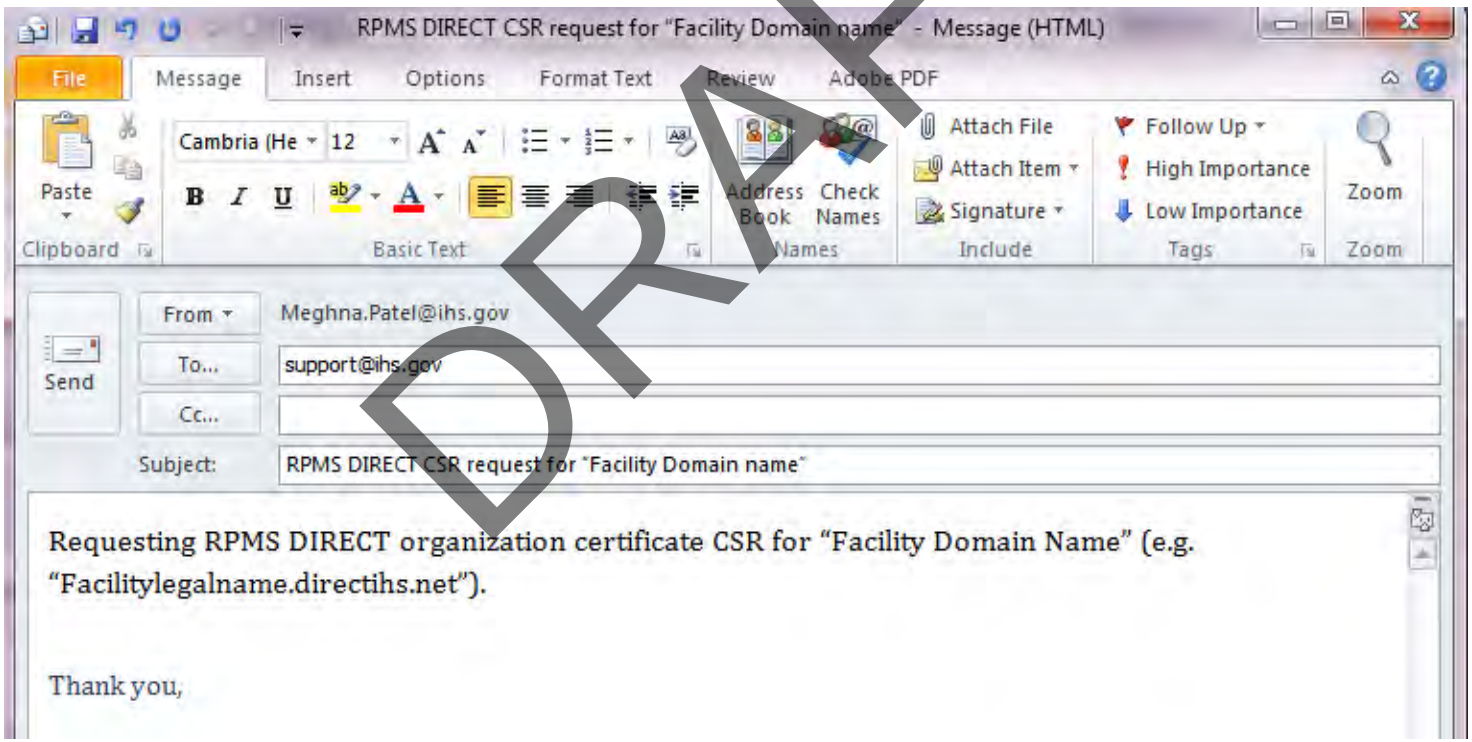
Add HCO

DRAFT

2. Complete requested information:
   - ❑ **Identity** section:
     - ❑ **Type** Field: *Organization*
     - ❑ **Health Care Organization:** *Facility's Legal Name*
     - ❑ **Address:** *Registered Address*
   - ❑ **Representative** Section:
     - ❑ MUST include the designated facility SU/FA information in the *Email, First Name, and Last Name field*
     - ❑ Check box for the *"Send contact info and authorization email".*
   - ❑ **Domain Info** section: *Facility's full domain name*
   - ❑ **Options** section:
     - ❑ **HIPAA Compliance Type** field: *HIPAA Covered Entity*
     - ❑ **Default Assurance Level** field: *Medium*
   - ❑ **Validation Options** section:
     - ❑ **When validating Order DigiCert should contact** field: *HISP Validation Contact*
     - ❑ **When validating Domains DigiCert should contact** field: *HISP Validation Contact*
   - ❑ Read & accept **Terms of Service**
   - ❑ Click on **CREATE HEALTH CARE ORGANZIATION** button at the bottom of the page.

Request Org. Certificate

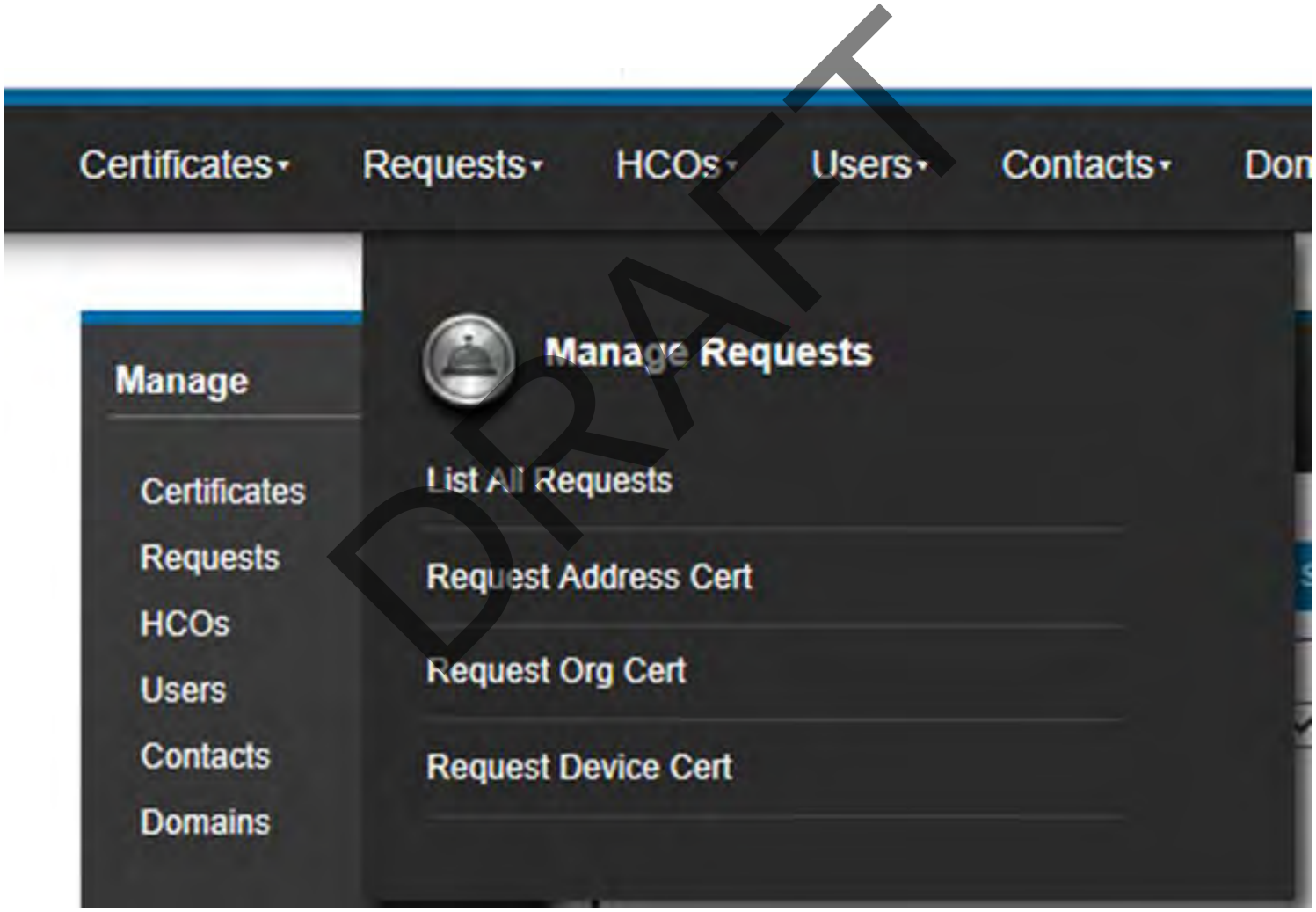
1. Complete Identity Proofing & upload Declaration Form for SU/FA
2. Update SU/FAs role to Trusted Agent
3. Request CSR for the facility domain name via OIT HD ticket from the RPMS DIRECT Development team at Support@ihs.gov:



DRAFT

Request Org. Certificate

4. From the CA Portal Main screen: Request → Request Org Cert

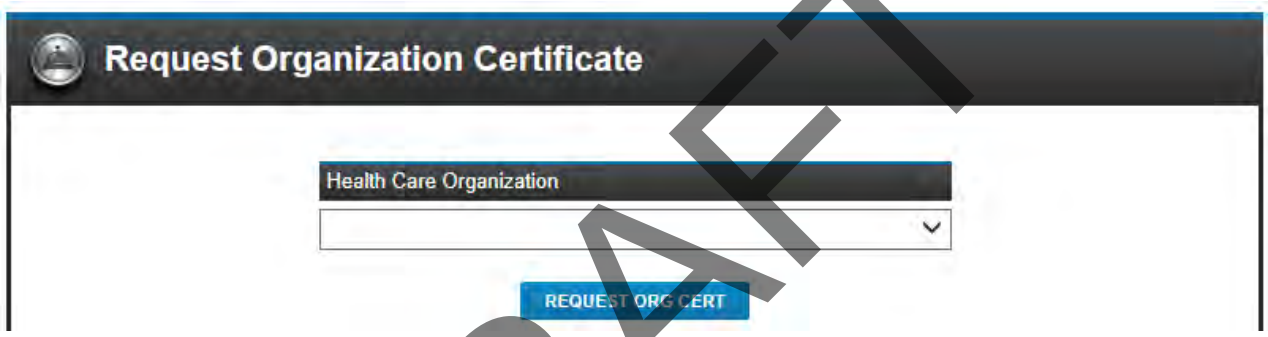


DRAFT

Request Org. Certificate

5. Select Facility's name for which organization certificate is being requested

- Click on the Request Org. Cert button

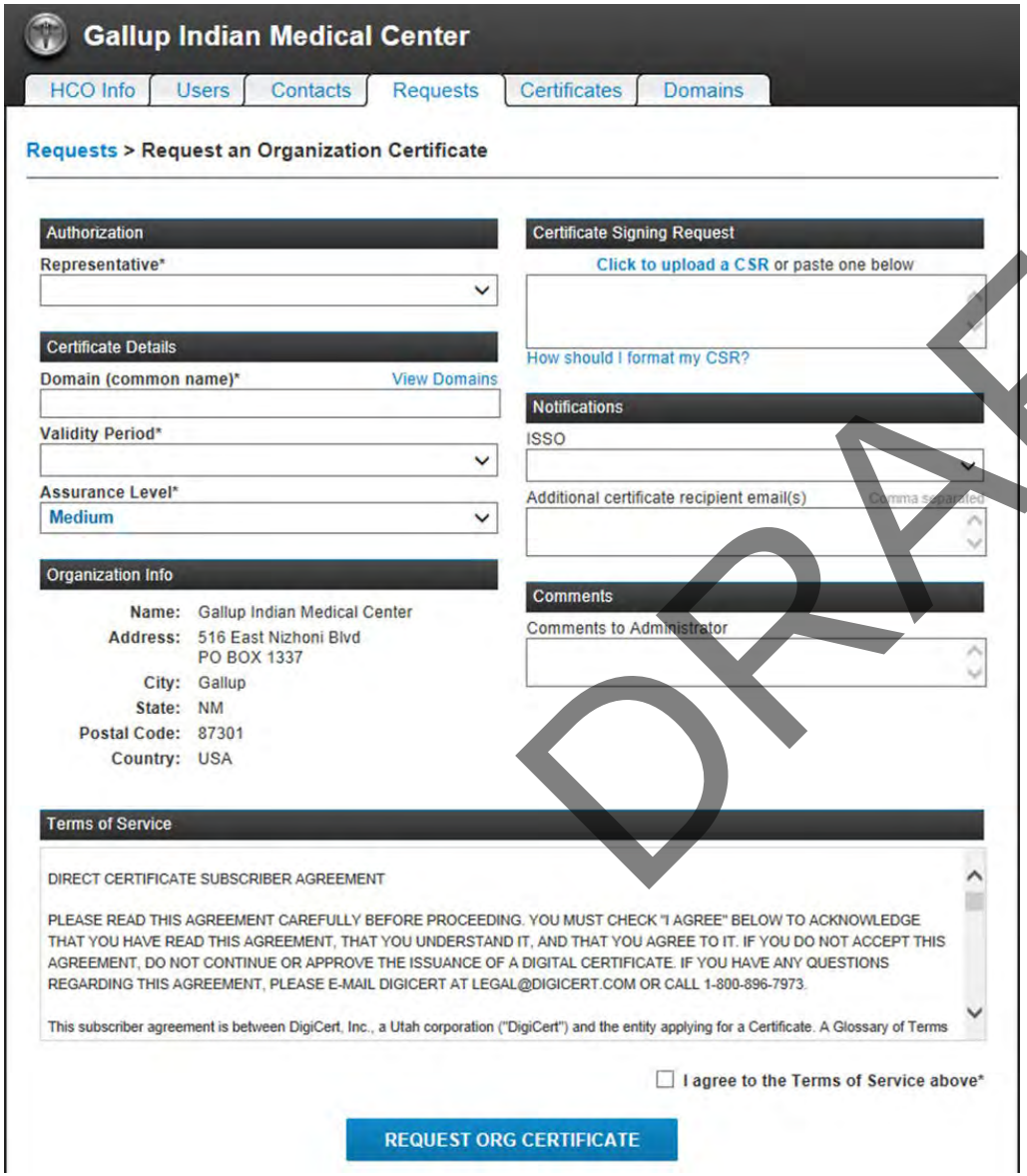


OR

When in the HCO screen click on the **Request ORG CERT** button

DRAFT

Request Org. Certificate



DRAFT

6. Complete Org Cert Request:

- ❑ **Representative:** This should be the HCO representative (RPMS DIRECT SU/FA) you added in the “Adding HCO”. Ensure that representative has submitted their Declaration form to complete the request.
- ❑ **Domain:** Enter the Facility’s Domain name for whom the certificate is being requested.
- ❑ **Validation Period**: 1 year
- ❑ **Assurance Level:** Medium
- ❑ **Certificate Signing Request (CSR):** Copy and paste CSR you received in step 3.
- ❑ **Notifications**: Select alternate AA name or enter their email under the Additional Certificate recipient email(s)
- ❑ Read and accept **Terms of Service**
- ❑ Click on **Request Org Certificate**

CSR

Important Note:

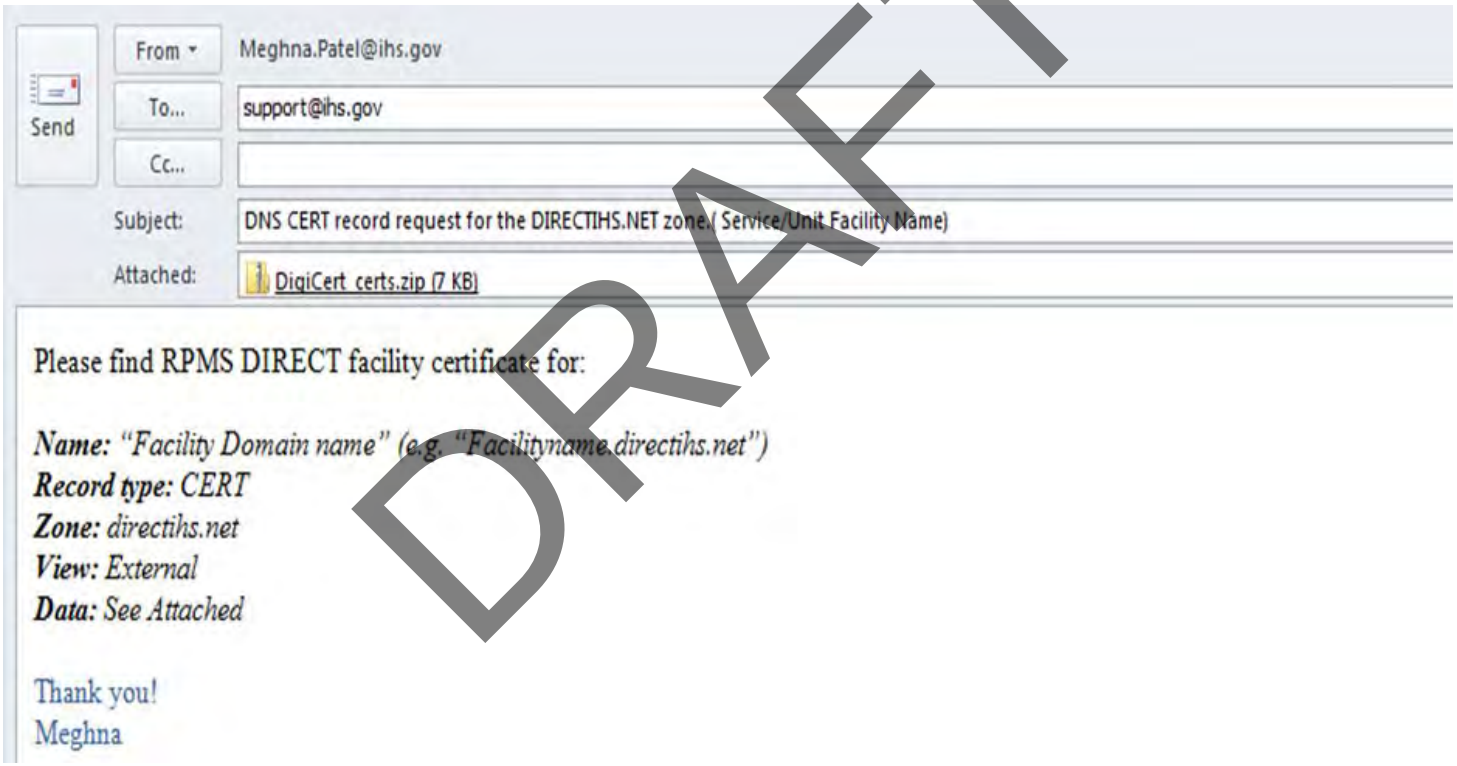
- Be sure to use CSR for the given Domain name
- When you paste the CSR in the box, make sure to include the first and last lines: **BEGIN CERTIFICATE REQUEST** and **END CERTIFICATE REQUEST** as illustrated below.

DRAFT

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxDTALBgNVBAgMBFV0YWgxDzANBgNV
BAcMBkxpbmRvbjEWMBQGA1UECgwNRGlnaUNlcnQgSW5jLjERMA8GA1UECwwIRGln
aUNlcnQxHTAbBgNVBAMMFGV4YW1wbGUuZGlnaWNlcnQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8+To7d+2kPWeBv/orU3LVbJwDrSQbeKamCmo
wp5bqDxIwV20zqRb7APUOKYoVEFFOEQs6T6gImnIolhbiH6m4zgZ/CPvWBOkZc+c
1Po2EmvBz+AD5sBdT5kzGQA6NbWyZGldxRthNLOs1efOhdnWFuhI162qmcflgpiI
WDuwq4C9f+YkeJhNn9dF5+owm8cOQmDrV8NNdiTqin8q3qYAHHJRW28glJUCZkTZ
wIaSR6crBQ8TbYNE0dc+Caa3DOIkz1EOsHWzTx+n0zKfqcbgXi4DJx+C1bjptYPR
BPZL8DAeWuA8ebudVT44yEp82G96/Ggcf7F33xMxe0yc+Xa6owIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAB0kcrFccSmFDmxox0Ne01UIqSsDqHgL+XmHTXJwre6D
hJSZwbvEtOK0G3+dr4Fs11WuUNt5qcLsx5a8uk4G6AKHMzuhLsJ7XZjgmQXGECpY
Q4mC3yT3ZoCGpIXbw+iP3lmEEXgaQL0Tx5LFl/okKbKYwIqNiyKWOMj7ZR/wxWg/
ZDGRs55xuoeLDJ/ZRFf9bI+IaCUd1YrfYcHIl3G87Av+r49YVwqRDT0VDV7uLgqn
29XI1PpVUNCPQGn9p/eX6Qo7vpDaPybRtA2R7XLKjQaF9oXWeCUqy1hvJac9QFO2
97Ob1alpHPoZ7mWiEuJwjBPii6a9M9G30nUo39lBi1w=
-----END CERTIFICATE REQUEST-----
```

Certificate Issuance & Mapping

7. DigiCert will validate organization and issue certificate
8. Email Certificate to ETS team for Mapping via email at Support@ihs.gov



DRAFT

9. Receive mapping confirmation from ETS

hMail Administrative Application

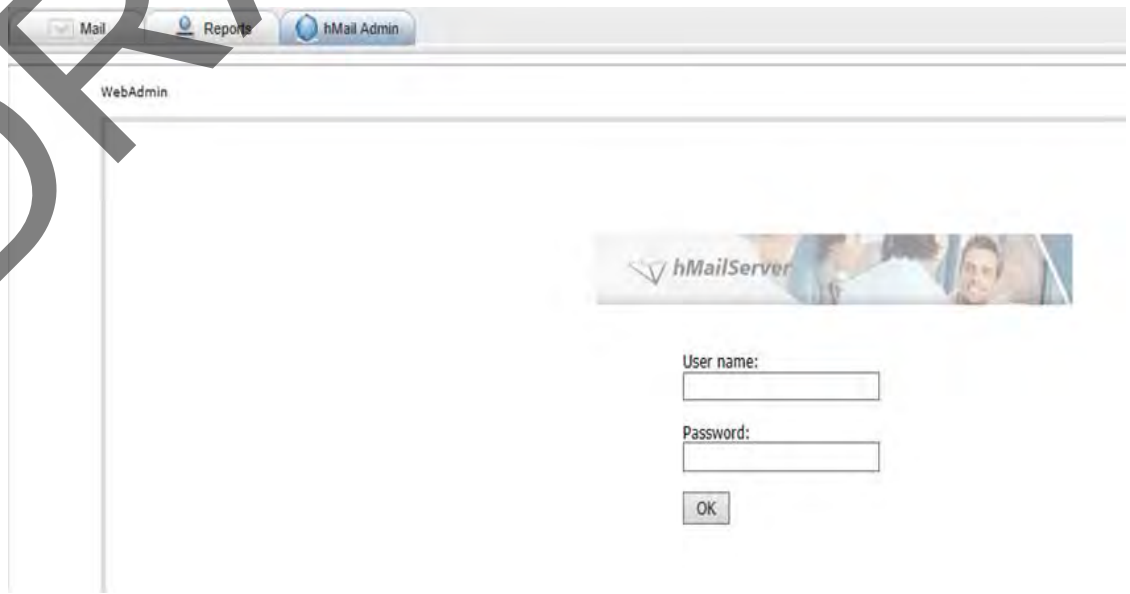
Access limited to:

- National Administrators
- Area Administrators
- Service Unit/Facility Administrators (SU/FA)

Functions:

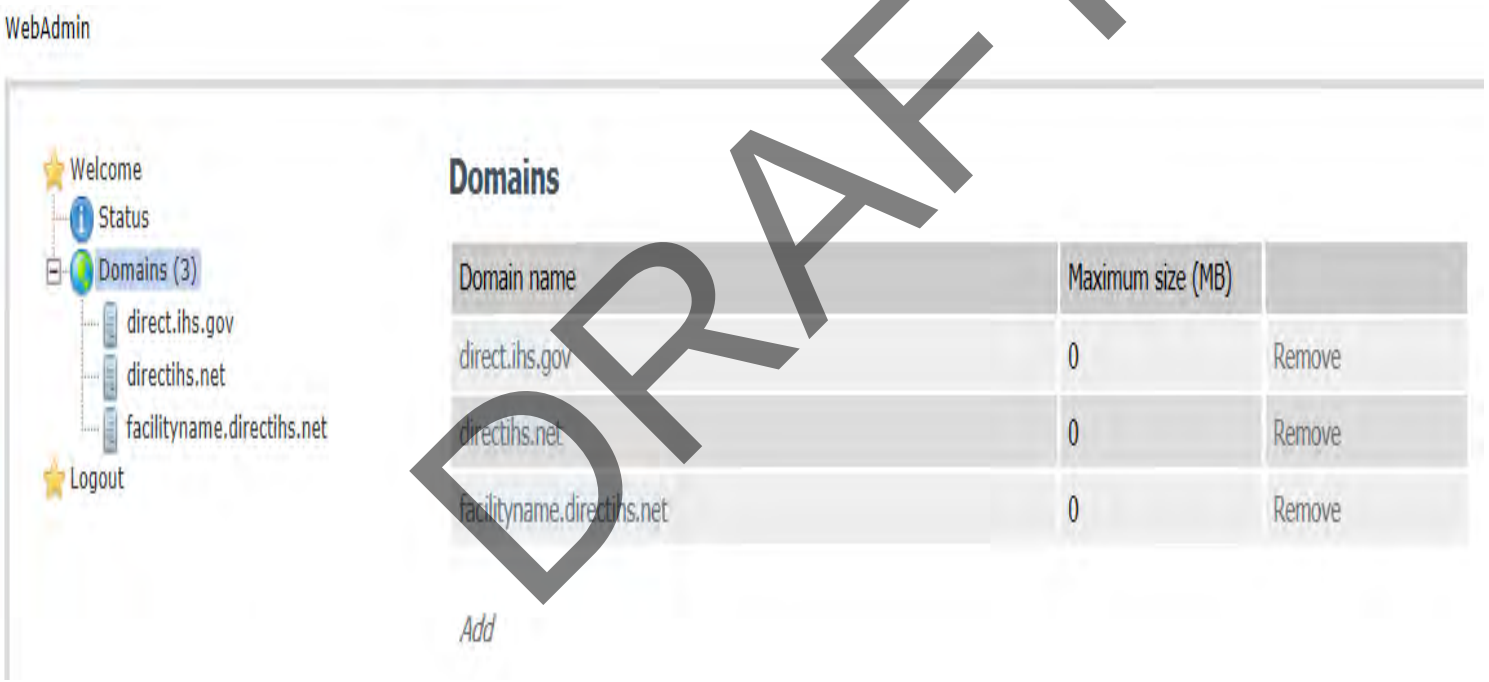
- Manage
  - Facility Domain Names
  - Users
  - User's Profile
  - Auto-reply
  - Message Forwarding

DRAFT



hMail: Add Domain

1. Add new Domain in the hMail Administrative Application

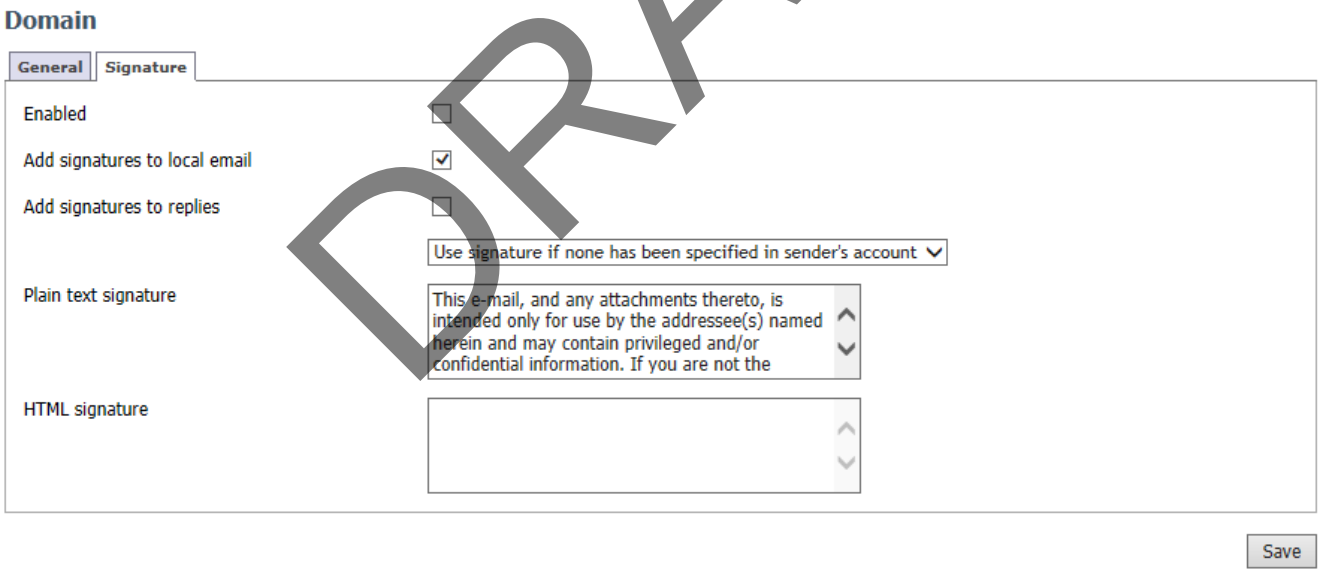


DRAFT

hMail: Add Domain

1a. General: Add facility's domain name

1b. Signature: Do <u>not</u> make any changes



DRAFT

1c. Save

hMail Administration Level

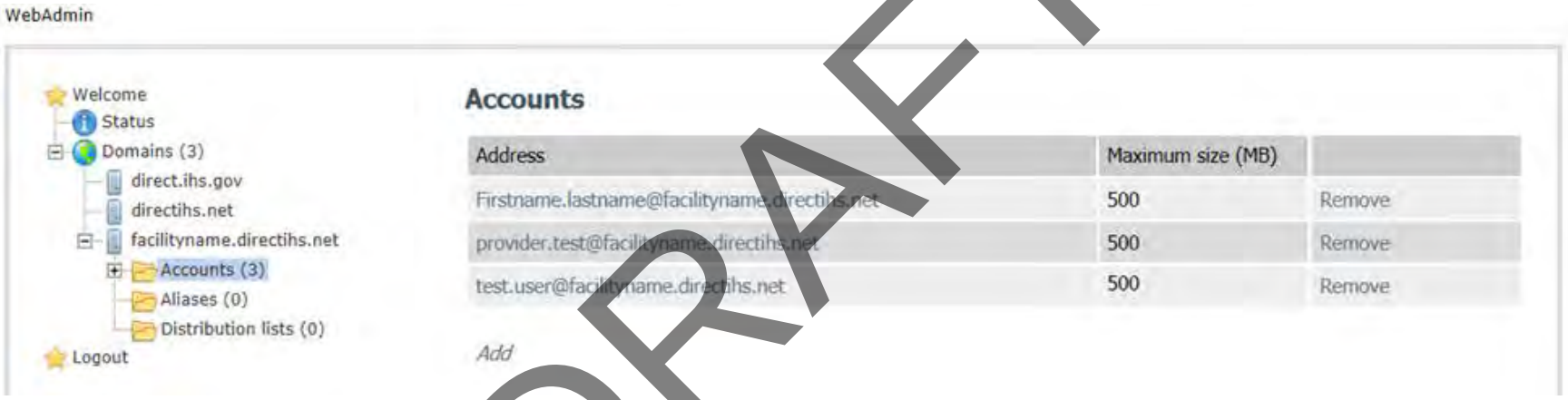
- Role designation within the hMail Administrative application.
- When setting up new Users and Administrator be sure to assign correct Administration Level.

RPMS DIRECT Messaging Role	Designated Administration level within RPMS DIRECT Administrative Application
National Administrator	Server
Area Administrator	Server
Service Unit/Facility Administrator	Domain
All None-Administrative Users: Message Agents, PHR Registrars, healthcare providers, healthcare staffs, and patients)	User

DRAFT

hMail: Add SU/FA

2. Add facility SU/FA in the hMail Administrative Application under their own domain.

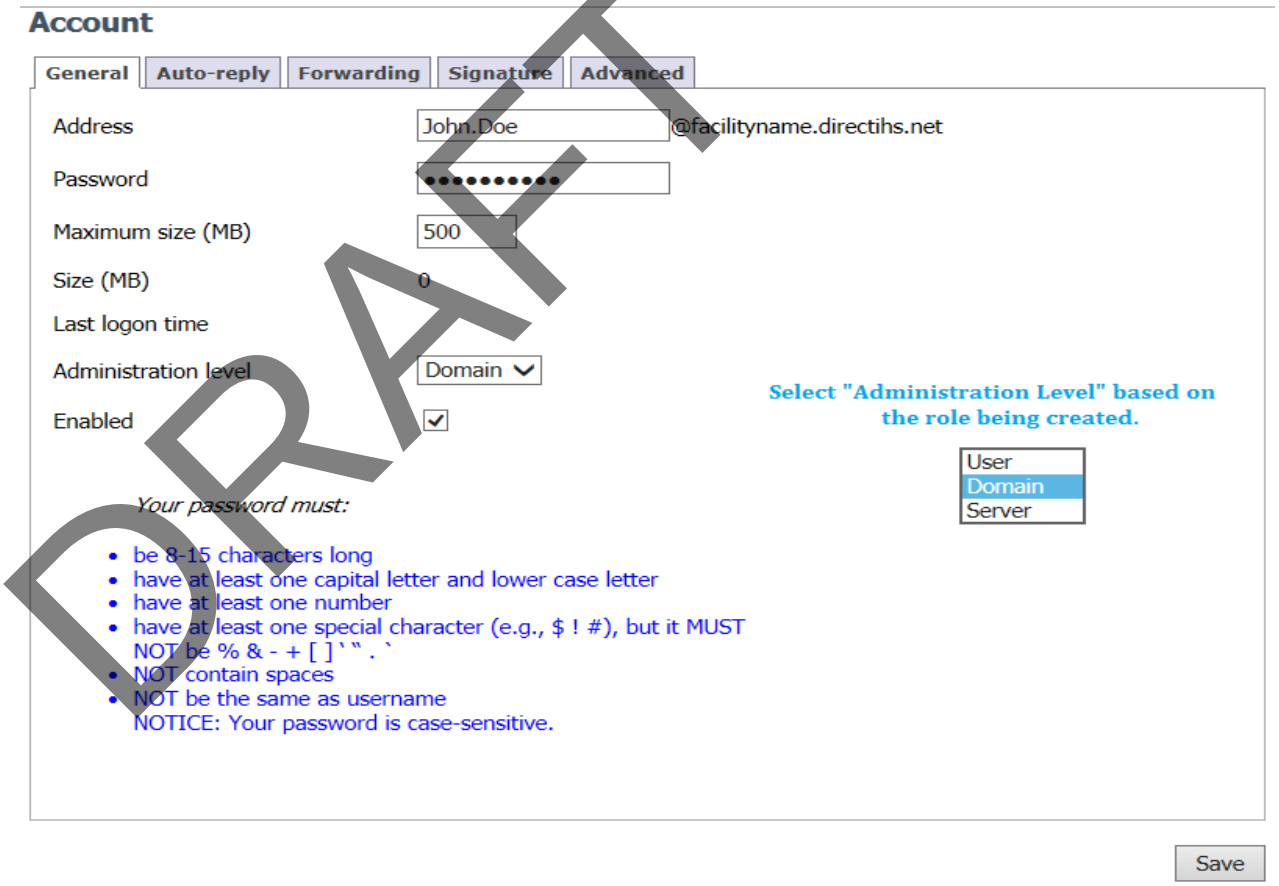


DRAFT

hMail: Add SU/FA

2a. General:

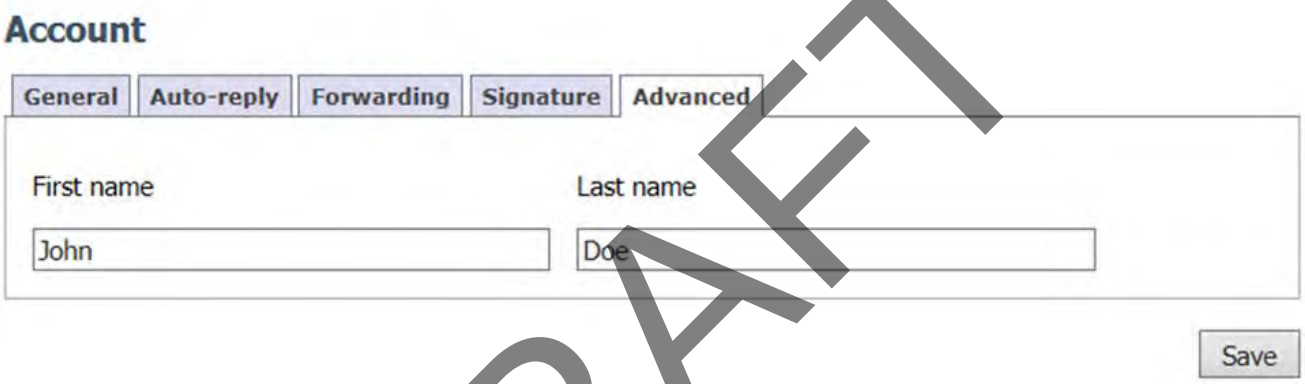
- **Address:** format must be *Firstname.lastname*
- **Password:** see requirement on the screen
- **Administration Level:** Select appropriate level based on the role



DRAFT

hMail: Add SU/FA

2b. Advanced: Add SU/FA's First and Last Name



2c. Save

3. Provide login credentials to the SU/FA

DRAFT

RPMS DIRECT Audits

Access limited to:

- National Administrators
- Area Administrators
- Service Unit/Facility Administrators (SU/FA)

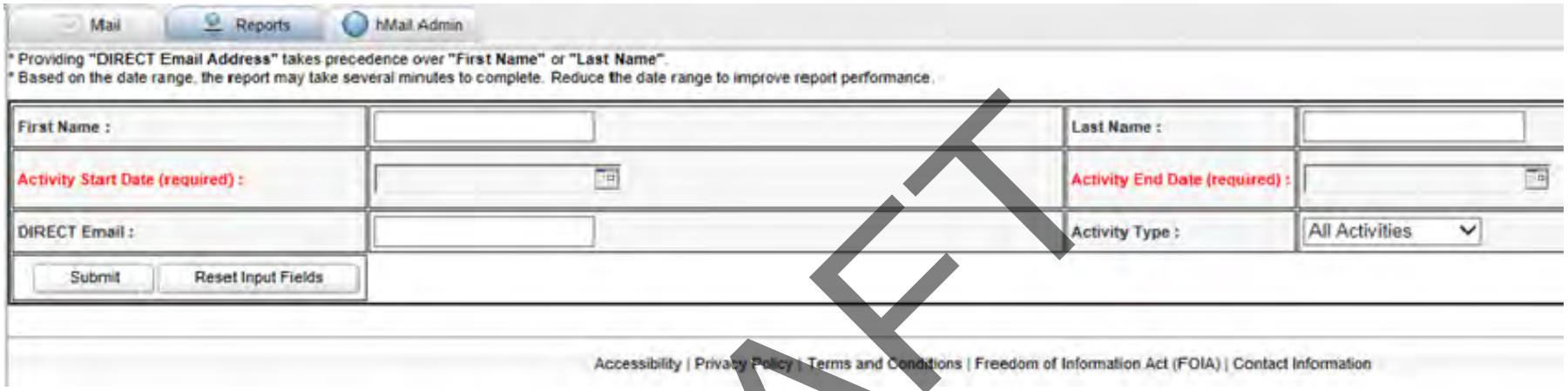
Functions:

- Auditing
  - Reactive Auditing
  - Proactive Auditing

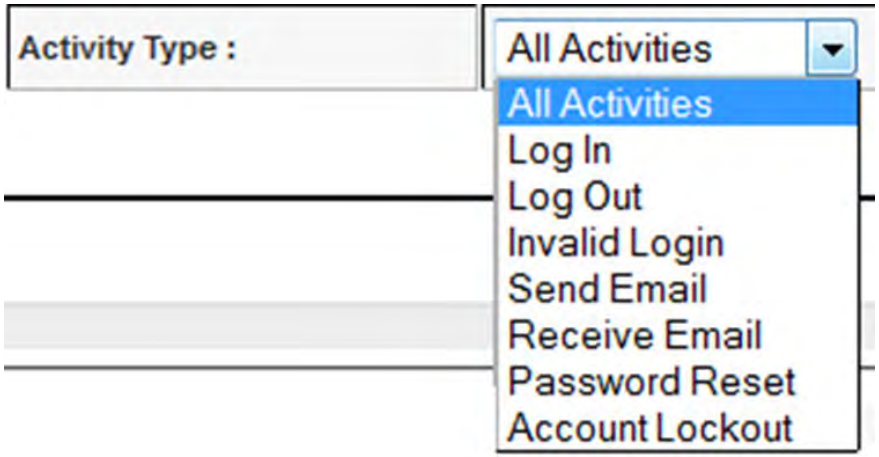
DRAFT

NOTE: See RPMS DIRECT Messaging Administrative Manual and Policy for more information

Audits



- Activity Start and end date is required
- Query by:
  - First name
  - Last name
  - Direct Email
  - Activity Type



DRAFT

Audit Report

- Sort Audit report
- Search through Audit report
- Export Audit Reports

First Name :		Last Name :	
Activity Start Date (required) :	2014-05-05	Activity End Date (required) :	2014-05-05
DIRECT Email :		Activity Type :	Send Email

Submit | Reset Input Fields

Show 10 | Search

Activity Date and Time	DIRECT Email Address	Message	Activity Type	First Name	Last Name
2014-05-05 07:17:19.0	mgreen@Facilityname.directihs.net	Send Email to 'mgrant mgrant@direct.ihs.gov' with subject 'An Important Message from your Healthcare Team' on '2014-05-05 07:17:19.0'	Send Email	null	null
2014-05-05 07:18:04.0	mgreen@Facilityname.directihs.net	Send Email to 'mgrant mgrant@direct.ihs.gov' with subject 'An Important Message from your Healthcare Team' on '2014-05-05 07:18:04.0'	Send Email	null	null
2014-05-05 07:18:08.0	mgreen@Facilityname.directihs.net	Send Email to 'mgrant mgrant@direct.ihs.gov' with subject 'An Important Message from your Healthcare Team' on '2014-05-05 07:18:08.0'	Send Email	null	null
2014-05-05 07:18:12.0	mgreen@Facilityname.directihs.net	Send Email to 'mgrant mgrant@direct.ihs.gov' with subject 'An Important Message from your Healthcare Team' on '2014-05-05 07:18:12.0'	Send Email	null	null
2014-05-05 07:24:09.0	mgreen@Facilityname.directihs.net	Send Email to 'mgrant mgrant@direct.ihs.gov' with subject 'Other' on '2014-05-05 07:24:09.0'	Send Email	null	null
2014-05-05 07:24:12.0	mgreen@Facilityname.directihs.net	Send Email to 'mgrant mgrant@direct.ihs.gov' with subject 'Other' on '2014-05-05 07:24:12.0'	Send Email	null	null

DRAFT

Next Step: Area Administrators

Area Administrators:

- Complete ITAC system for PHR and RPMS DIRECT access request
- Obtain ITAC training and access
- Complete DigiCert Declaration Form
- Identify PHR and RPMS DIRECT early adopters
- Identify early adopters' SU/FA
- Train early adopters' SU/FA
- Submit Readiness Assessment Form by 8/22

DRAFT

Note:
PHR & RPMS DIRECT Beta Area Office will receive Deployment package by 8/13 COB All other Areas will receive post Beta test period

Next Step: SU/FA

Service Unit/Facility Administrators:

- Complete ITAC system for PHR and RPMS DIRECT access request
- Complete DigiCert Declaration Form
- Identify local team
  - PHR Registrars
  - Message Agents
  - Facility Address Designee
  - CAC's
- Train local team
- Submit Readiness Assessment Form by 8/22

DRAFT

Note:
PHR & RPMS DIRECT Beta Area Office will receive Deployment package by 8/13 COB All other Areas will receive post Beta test period

More Information

Additional Resources:

- Pre-Deployment Guide
- User and Administrator Manuals
- Policies
- Flyers for Outreach
- Readiness Assessment Form
- Declaration Form

Training for Areas and Early Adopters

- **Subject:** Central Services PHR & RPMS DIRECT registration and user training for Area and early adopters
- **Date:** August 27th, 2014
- **Time:** 12pm-2:30pm EST (11am CT, 10am MT, 9am PT)

Note:
PHR & RPMS DIRECT Beta Area Office will receive Deployment package by 8/13 COB All other Areas will receive post Beta test period

DRAFT

Questions and Discussion

DRAFT