



First Responder Communities of Practice - Rules of Behavior

First Responder Communities of Practice is an information technology service established by the Department of Homeland Security (DHS) Science & Technology Directorate's First Responder Technologies (R-Tech) program.

First Responder Communities of Practice provides First Responders access to an online collaborative platform to share information, network with other vetted First Responders and collect and share resources relevant to prevent, protect against, respond to and recover from all-hazard incidents. Because the service may provide sensitive but unclassified information, access to the Service is limited to members who have been identified and authorized by First Responder Communities of Practice.

While the site's landing page is available to the general public on the Internet (via any compatible web browser), privileged access is restricted to those individuals who have been vetted and authorized by First Responder Communities of Practice personnel, and subsequently identified and authenticated by the system itself via a user logon and password.

Registered Users should be aware that by registering they have implicitly provided permission for the system to send them periodic service announcements and administrative messages via email.

Registered Users should also understand and agree that the service may include certain communications from First Responder Communities of Practice personnel. User information will not be used for marketing purposes or shared except if required by applicable DHS policy or federal laws or regulations.

DHS 4300A Sensitive Systems Policy requires system specific Rules of Behavior (RoB) to be defined for all DHS IT systems. This RoB policy details the expected behavior of Registered Users when accessing and using the system. RoB policies that are understood and followed help ensure the security of systems and the confidentiality, integrity, and availability of information. RoB policies inform users of their responsibilities and let them know they will be held accountable for their actions while they are accessing DHS owned systems. DHS 4300A Sensitive Systems Policy requires that Registered Users are briefed with regards to these rules and are aware of the disciplinary actions that may result from non-compliance. Additionally, Users are required to agree to and sign this RoB policy (done via a checkbox during registration) prior to being granted Registered User access to the First Responder Communities of Practice.

The First Responder Communities of Practice Information Systems Security Officer (ISSO) will ensure that all Registered Users read and acknowledge the RoB before being granted access to the system. The ISSO, in conjunction with System and Application Administrators as appropriate, will maintain a current list of all registered First Responder Communities of Practice users and ensure that evidence of

acknowledgement of the RoB are on file for each. Acknowledgement of the RoB is captured when a registering user clicks the checkbox stating "I have read and understand the Rules of Behavior".

All Non-Compliances with the First Responder Communities of Practice RoB shall be considered security incidents in accordance with DHS policy and thoroughly investigated by the system's ISSO in accordance with the First Responder Communities of Practice Incident Response Plan. If an investigation concludes that a violation has indeed occurred, a warning may be issued, or the offending Registered User's account may be temporarily or permanently disabled or removed, effectively revoking all privileged access to the information system and any data contained therein. In some cases, violators may be subject to criminal prosecution.

The following RoB shall be strictly adhered to by all First Responder Communities of Practice Registered Users. The First Responder Communities of Practice is subject to change at any time. If the RoB does change, Registered Users will be notified by email and asked to re-read and re-acknowledge or risk the temporary disablement of their account at the discretion of the First Responder Communities of Practice ISSO, until they comply.

User Account:

- Registered Users shall be provided access and granted rights to First Responder Communities of Practice according to "need to know" and "least privilege".
- Users shall understand that any/all use of the First Responder Communities of Practice information system is subject to continuous monitoring in accordance with DHS policy at that access is at the liberty of DHS.
- Users shall not circumvent or attempt to circumvent any security countermeasures or safeguards.
- All users shall have individual accounts. Shared, or sharing of, accounts shall not be permitted at any time, for any reason.
- All user account credentials (usernames and passwords) will be unique and associated directly with a single "live" individual.
- No individual user shall be permitted more than one account at any given time.
- Users shall be aware that their account is subject to automatic disablement after 45 days of
 inactivity. Users will be sent a warning notice when their account is about to be disabled.
- If an individual user no longer requires access to First Responder Communities of Practice, it shall be his or her responsibility to notify the system's ISSO or System Administrator immediately so that the account can be disabled or removed.
- User accounts/credentials shall not be transferrable to any other individual under any circumstances.

Password Protection:

- Users shall protect their password from disclosure.
- Users shall not reveal their password to others.
- Users shall be responsible for any computer activity associated with their username and password.
- User shall not write down or post their password
- Users shall change their password immediately if it is suspected to have been compromised and subsequently notify the First Responder Communities of Practice ISSO and/or System Administrator.
- All passwords shall meet the following password requirements:
 - Passwords are at least 8 characters long and have a combination of letters (upper- and lower-case), numbers, and special characters. Null passwords are not allowed.
 - Passwords must be changed every 90 days and the new password cannot be the same as any of the user's last eight passwords.

System Access:

- Users shall not enter into this or any other DHS computer system without explicit authorization.
 Any unauthorized entry into this information system is a serious security violation and may result in civil or criminal prosecution depending on the extent of the violation.
- Users shall not permit any unauthorized individual (including spouse, relative, co-worker, or friend) access to restricted/non-public areas of the information system.
- Users shall understand and accept responsibility for protecting all output generated under their

- account (for example, printed output, CD/DVD ROM, USB/Flash memory, external hard drives, magnetic tapes).
- Users shall not print, distribute or disseminate other users' Personally Identifiable Information.
- Users shall understand and accept that there is no expectation of privacy and that their activity is subject to auditing at all times while using First Responder Communities of Practice.
- Users shall agree to notify the System Administrator when access to the information system is no longer needed or when a user ceases to be a First Responder.
- Users shall understand that evidence of acknowledgement of this agreement will be kept on file with the System Administrator when they agree to accept the RoB.

Website Content:

- Information or content posted to the website must relate to professional activities and mission of First Responder Communities of Practice.
- Users shall not upload, post, email, transmit or otherwise make available any content that is
 unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene,
 libelous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable.
- Users shall not post CLASSIFIED or LAW ENFORCEMENT SENSITIVE information or
 documents to the First Responder Communities of Practice under any circumstance. In addition,
 it is the user's responsibility to use reasonable judgment when posting data to the system to avoid
 the creation of information that could be considered SENSITIVE of CLASSIFIED in aggregate.
 Only FOR OFFICIAL USE ONLY or SENSITIVE BUT UNCLASSIFIED MATERIAL is permitted on
 the site.
- Users shall not impersonate any person or entity, or falsely state or otherwise misrepresent themselves or any data they put on the system.
- Users shall not forge headers or otherwise manipulate identifiers in order to disguise the origin of any content transmitted through First Responder Communities of Practice.
- Users shall not upload, post, email, transmit or otherwise make available any content that you do
 not have a right to make available under any law or under contractual or fiduciary relationships
 (such as inside information, proprietary and confidential information learned or disclosed as part

of employment relationships or under nondisclosure agreements).

- Users shall not upload, post, email, transmit or otherwise make available any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party.
- Users shall not upload, post, email, transmit or otherwise make available any unsolicited or unauthorized advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes," or any other form of solicitation.
- Users shall not upload, post, email, transmit or otherwise make available any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment; interfere with or disrupt the Service or servers or networks connected to the Service, or disobey any requirements, procedures, policies or regulations of networks connected to the Service; intentionally or unintentionally violate any applicable local, state, national or international law; collect or store personal data about other users.

Security Reporting Requirements:

Registered Users must promptly report any known/observed violations of or non-compliance with the First Responder Communities of Practice RoB including (but not limited to) observed IT security incidents, suspicions of security violations, or posting of inappropriate content. Reports should be made directly to the First Responder Communities of Practice ISSO or System Administrator.

Export Control

First Responder Communities of Practice is a tool to share industry-specific information, including both technical and non-technical information, among practitioners and interested parties. It is the user's responsibility to comply with all applicable laws and regulations regarding the export of controlled information. Exporting information includes providing access to information through emails, links, and other sharing mechanisms. Certain information, including technical data such as that which is available on this website, may be controlled for export reasons, including through email, from the United States or, within the United States, to foreign nationals.

For further guidance, please see www.pmddtc.state.gov or www.bis.doc.gov.

Modification of the Service

First Responder Communities of Practice reserves the right at any time to modify or discontinue, temporarily or permanently, the Service (or any part thereof) with or without notice. You agree that First Responder Communities of Practice shall not be liable to you or to any third party for any modification, suspension or discontinuance of the Service. First Responder Communities of Practice is not liable for any data or information lost as a result of discontinuance of service.

Termination

You agree that First Responder Communities of Practice may, under certain circumstances and without prior notice, immediately terminate your account and access to the Service. Cause for such termination shall include, but not be limited to, (a) breaches or violations of the RoB or other incorporated agreements or guidelines, (b) requests by law enforcement or other government agencies, (c) a request by you (self-initiated account deletions), (d) discontinuance or material modification to the Service (or any part thereof), (e) unexpected technical or security issues or problems, and (f) extended periods of inactivity. Termination of your First Responder Communities of Practice account may include (a) deletion of your password and all related information, files and content associated with or inside your account (or any part thereof) and (b) barring further use of the Service. Further, you agree that all terminations for cause shall be made in First Responder Communities of Practice sole discretion and that First Responder Communities of Practice shall not be liable to you or any third party for any termination of your account or access to the Service.

Links

The Service or authorized users may provide links to other World Wide Web sites or resources. Because First Responder Communities of Practice has no control over such sites and resources, you acknowledge and agree that First Responder Communities of Practice is not responsible for the availability of such external sites or resources and does not endorse and is not responsible or liable for any content, advertising, products, or other materials on or available from such sites or resources. You further acknowledge and agree that First Responder Communities of Practice shall not be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such Content, goods or services available on or through any such site or resource.

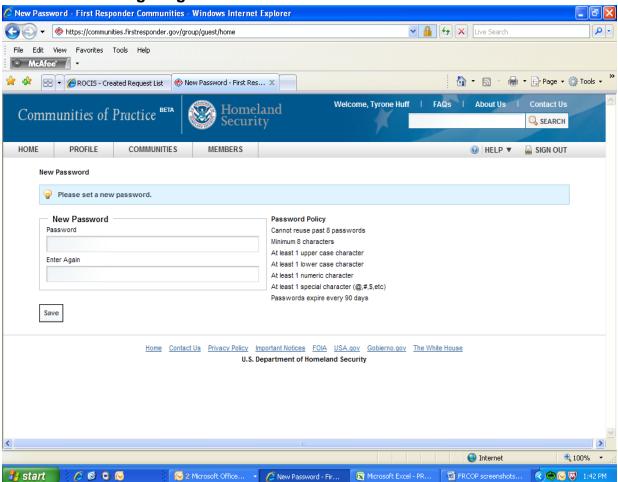
Acknowledgment Statement

- I understand that I have no expectation of privacy while using First Responder Communities of Practice.
- I understand that I will be held accountable for my actions while accessing and using First Responder Communities of Practice.
- I agree to indemnify and hold First Responder Communities of Practice and its subsidiaries,

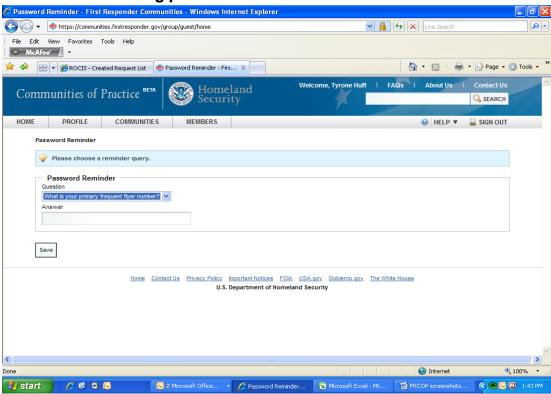
affiliates, officers, agents, co-branders or other partners and employees harmless from any claim or demand, including reasonable attorneys' fees, made by any third party due to or arising out of content I submit, post, transmit or make available through the Service, my use of the Service, my connection to the Service, my violation of the Rules of Behavior, or my violation of any rights of another.

- I acknowledge that I have received as well as understand my responsibilities and will comply with the Rules of Behavior for the First Responder Communities of Practice system.
- As a Registered User of First Responder Communities of Practice, I acknowledge my
 responsibility to conform to the above requirements set forth the by the Communities of Practice
 Program on behalf of the Department of Homeland Security's Science & Technology Directorate.
 I understand that my failure to agree to these Rules of Behavior will result in denial of access to
 Communities of Practice and its system components.

Screen after hitting "I agree"



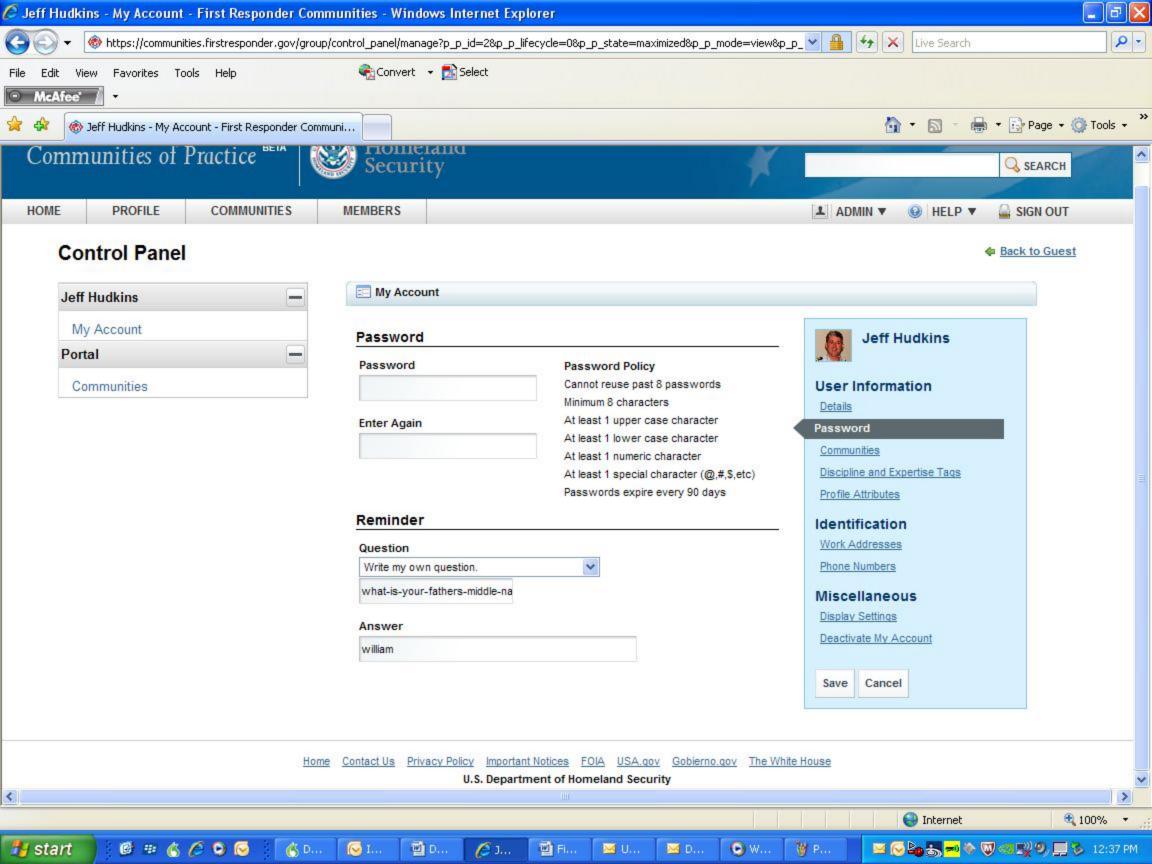
Screen after resetting password:

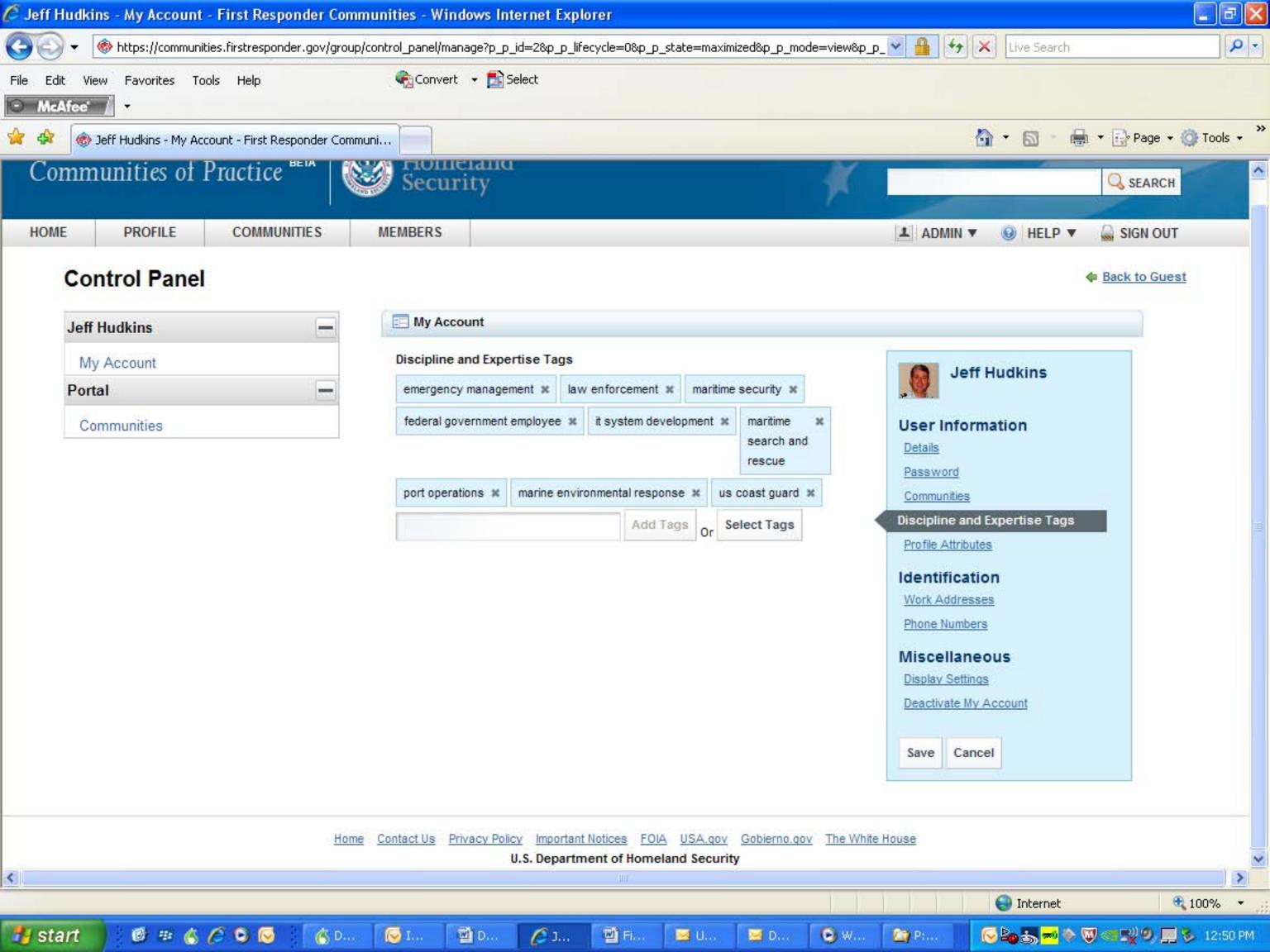


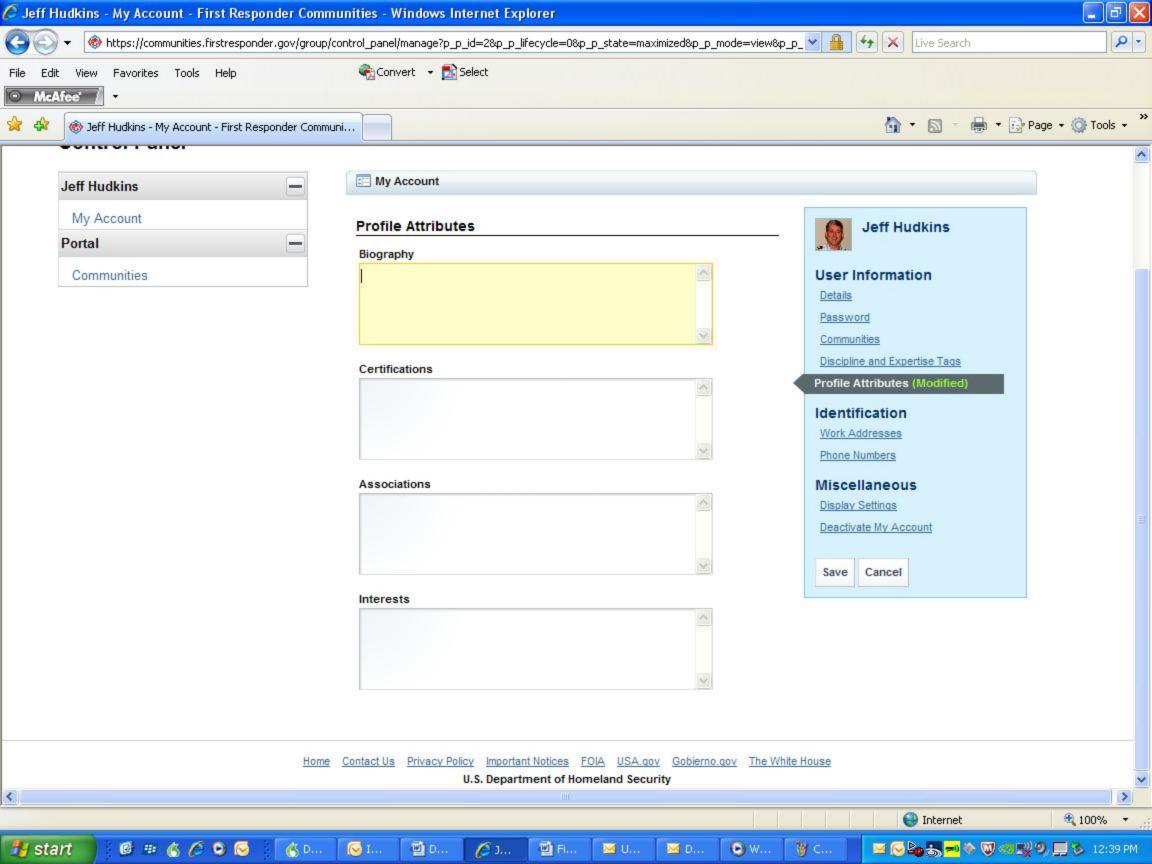
First Page after you pass the log in and password pages:

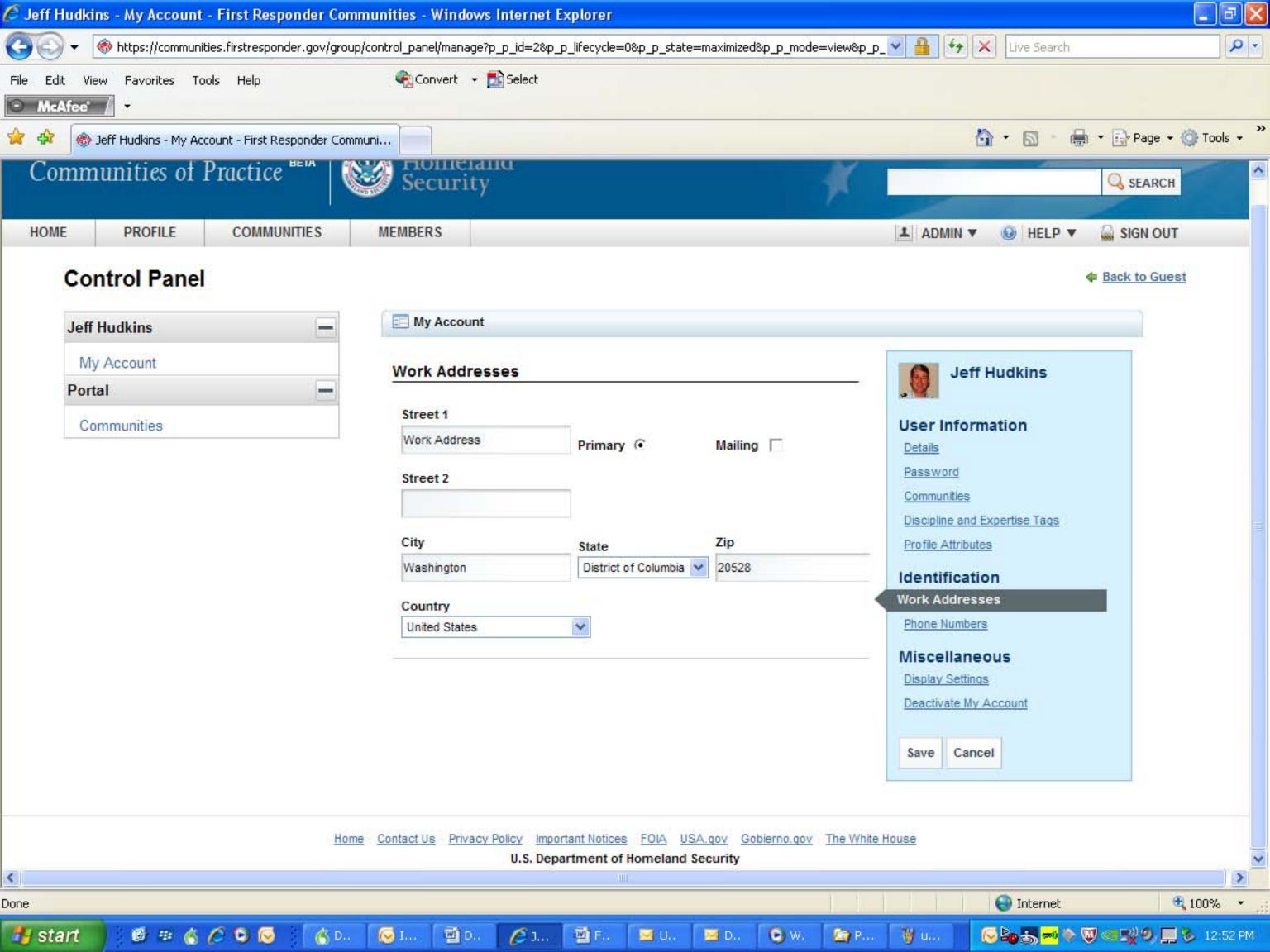


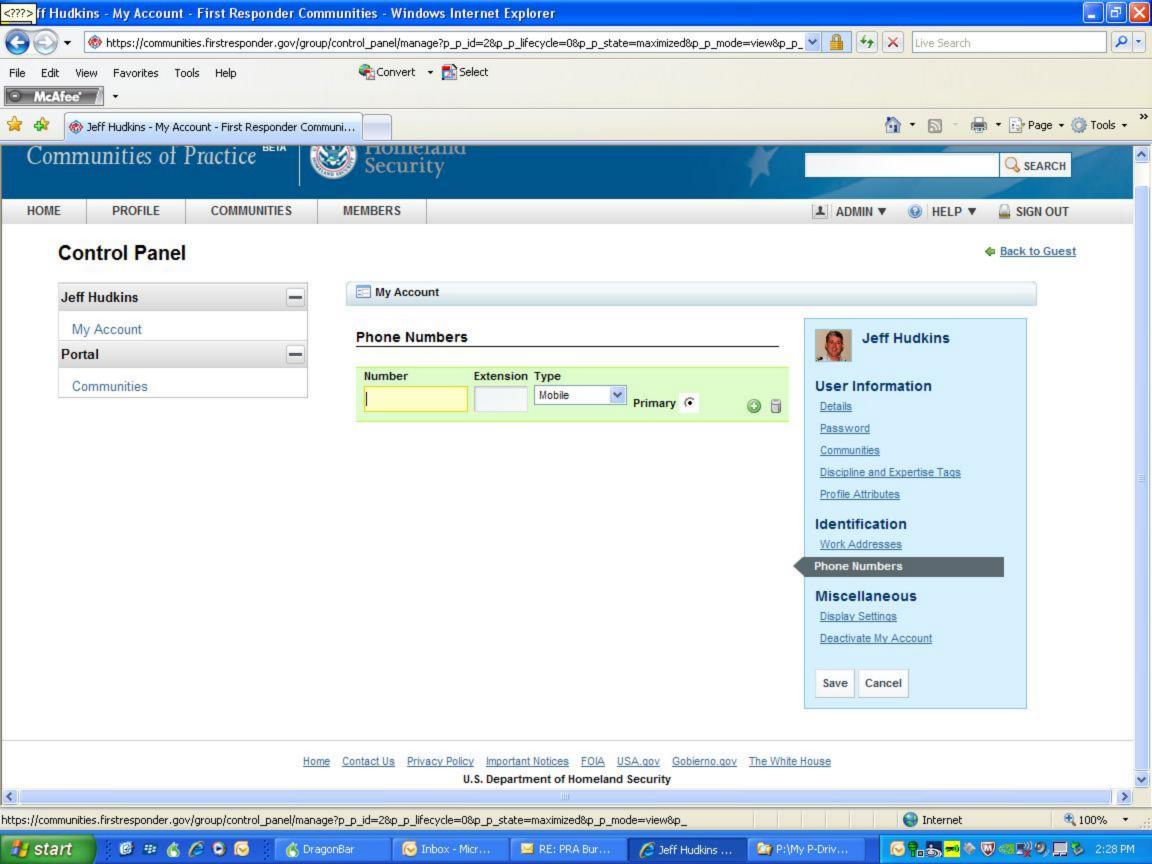


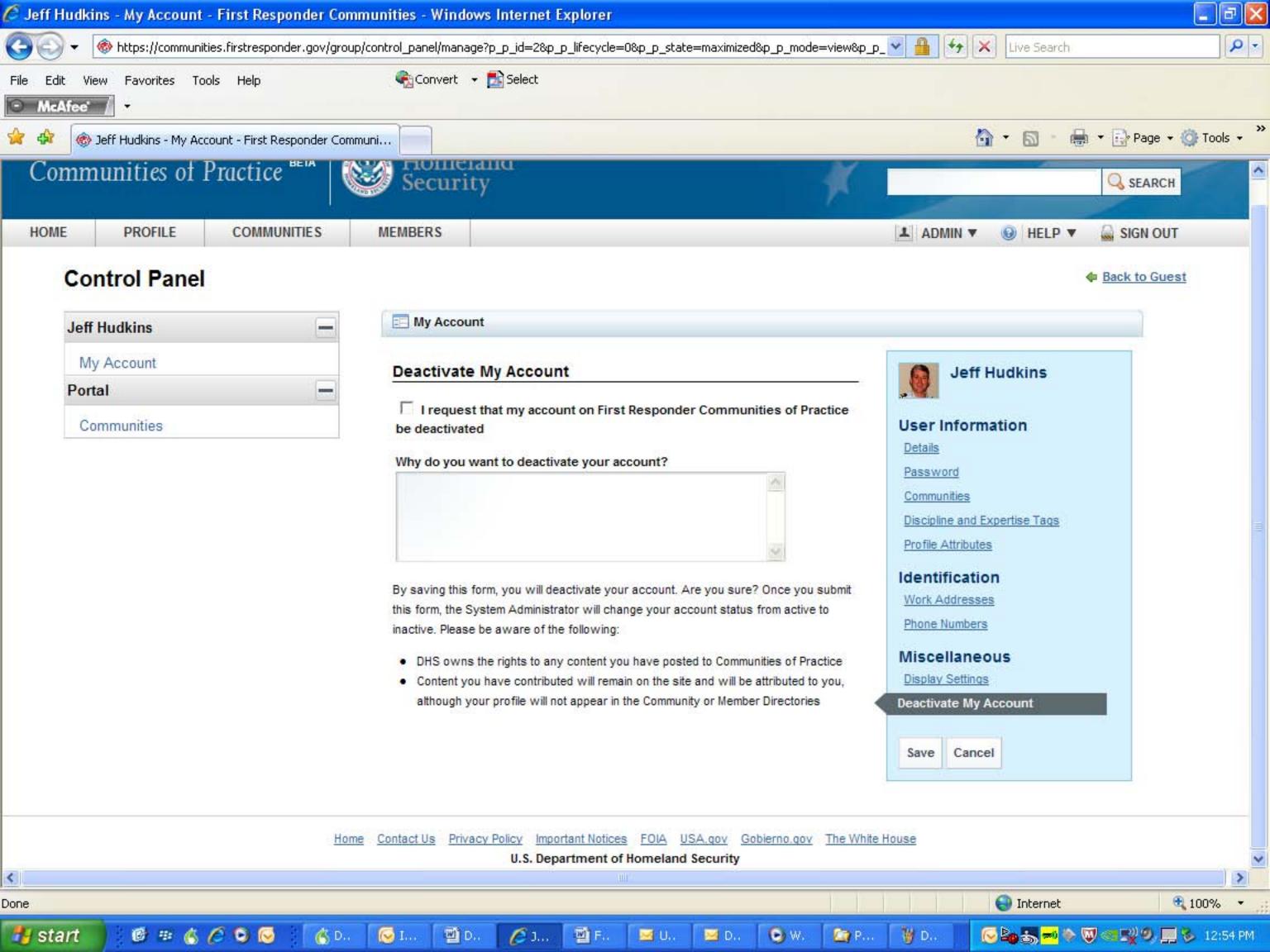










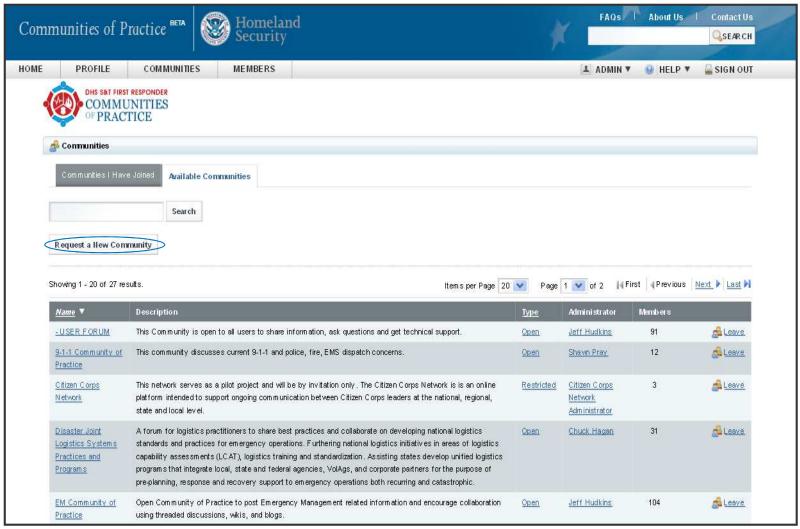


Home Page



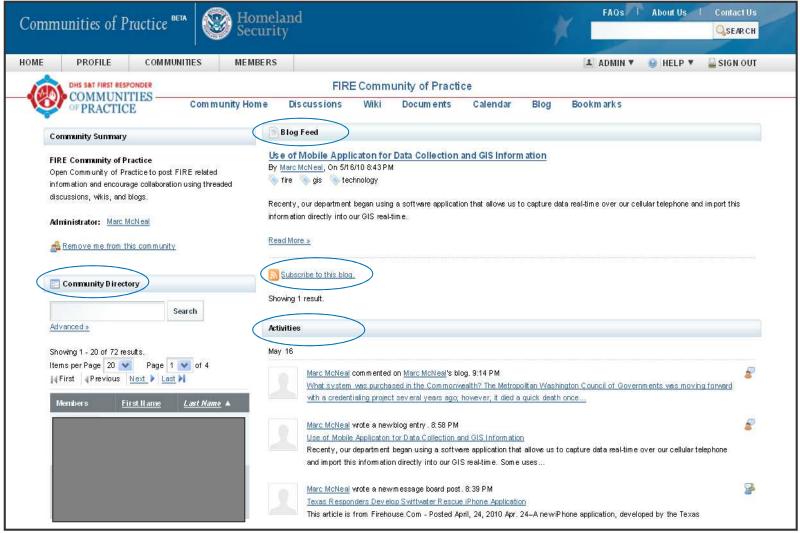


Available Communities



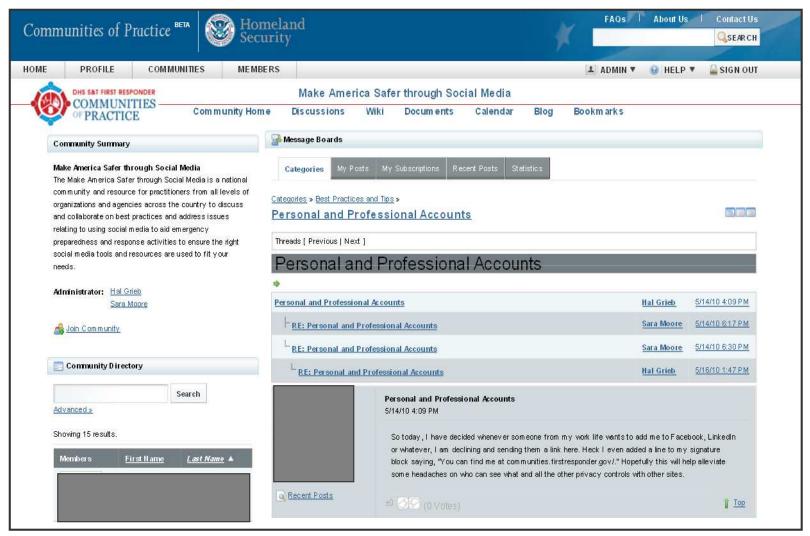


Community Home Page



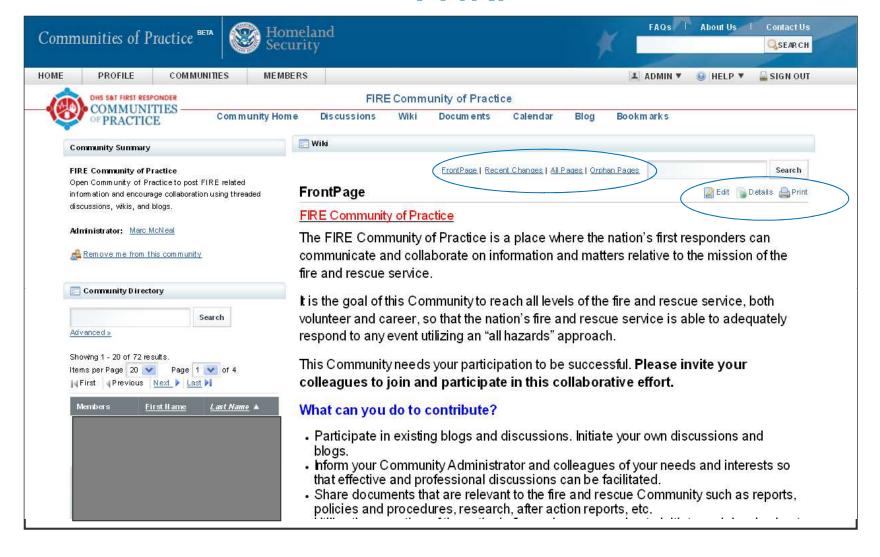


Discussion Board



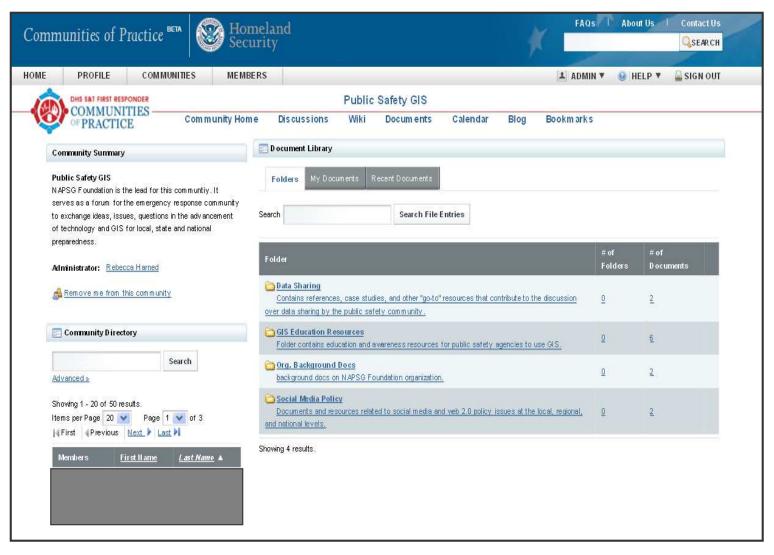


Wiki



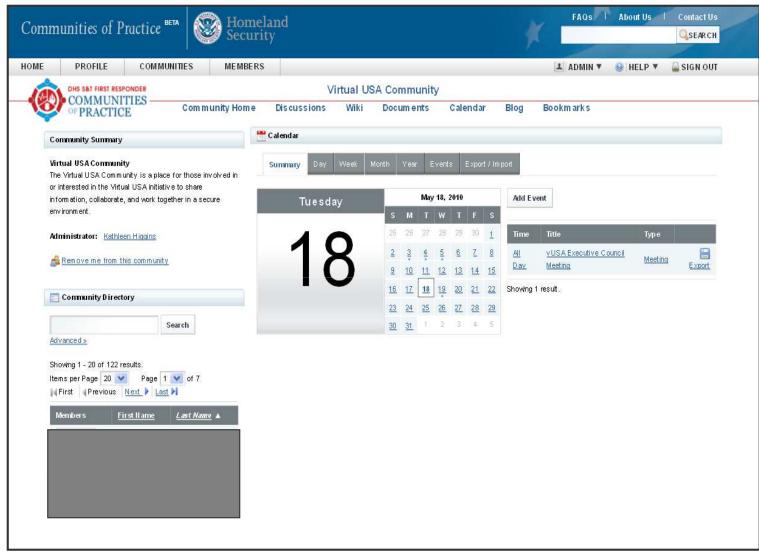


Documents





Shared Calendar





Bookmarks

