

## WOC Packet Checklist

### 1. WOC Letter

\_\_\_\_\_ Print your name at the top after the word "DEAR"

\_\_\_\_\_ Read the Form.

\_\_\_\_\_ Sign and date at the bottom of the form.

### 2. Declaration for Federal Employment

\_\_\_\_\_ Read Page 1 and complete the answers on page 2 and 3.

\_\_\_\_\_ Remember to provide a response in box 16 for any questions you may have answered yes to on page 2 or 3 of this document.

### 3. Application for Health Professions Trainees (VA Form 10-2850d)

\_\_\_\_\_ Complete all sections of the form with the exception of **section IV (4)**

\_\_\_\_\_ Insure that your name and SSN is listed at the top of each page of the form

\_\_\_\_\_ You must sign the bottom of page 3 and the center of page 4 (2 signatures on this form)

### 4. INS Form I-9, Employment Eligibility Verification

\_\_\_\_\_ Complete "Section 1". Be sure to date and sign that section.

\_\_\_\_\_ Refer to the reference page (page 2) to determine what form of ID you will present to the VA staff on the day of your appointment (processing). If you choose something from Column A that is all you will need.

If you choose a document from Column B it **MUST** be accompanied by a document from Column C.

If you were not born in the United States but are a naturalized US citizen please bring your original naturalization documentation or a US passport (if you have one) with you.

**5. Department of Veterans Affairs (VA) National Rules of Behavior**

\_\_\_\_\_ Please read and sign this document

**6. Electronic Questionnaire for Investigations Processing (e-QIP)**

\_\_\_\_\_ READ ***before*** attempting to enter your data in to the computer.

\_\_\_\_\_ Under “Web Browser Requirements” follow appropriate TLS instructions to ensure confidentiality. Most of you will use the directive listed for enabling TLS for “Internet Explorer”.

\_\_\_\_\_ Be sure to **print out both the release form and the certification form** when you finish entering your data. Then be sure to complete the process and **“Release the File to Agency”**. This should provide you with a final screen which states the word **“Farewell”** in the upper left corner of the page.

**7. SAC Sheet**

\_\_\_\_\_ Fill out all spaces on the fingerprint (SAC) form.

**8. The day of your appointment (processing).**

\_\_\_\_\_ Bring all of your completed forms with you.

\_\_\_\_\_ Bring whatever ID Forms(s) you have chosen to present as listed on the back of the I-9 form.

\_\_\_\_\_ Bring the printed certification and release pages with you.

# Declaration for Federal Employment

Form Approved:  
OMB No. 3206-0182

## Instructions

The information collected on this form is used to determine your acceptability for Federal and Federal contract employment and your enrollment status in the Government's Life Insurance program. You may be asked to complete this form at any time during the hiring process. Follow instructions that the agency provides. If you are selected, before you are appointed you will be asked to update your responses on this form and on other materials submitted during the application process and then to recertify that your answers are true.

All your answers must be truthful and complete. A false statement on any part of this declaration or attached forms or sheets may be grounds for not hiring you, or for firing you after you begin work. Also, you may be punished by a fine or imprisonment (U.S. Code, title 18, section 1001).

Either type your responses on this form or print clearly in dark ink. If you need additional space, attach letter-size sheets (8.5" X 11"). Include your name, Social Security Number, and item number on each sheet. We recommend that you keep a photocopy of your completed form for your records.

## Privacy Act Statement

The Office of Personnel Management is authorized to request this information under sections 1302, 3301, 3304, 3328, and 8716 of title 5, U. S. Code. Section 1104 of title 5 allows the Office of Personnel Management to delegate personnel management functions to other Federal agencies. If necessary, and usually in conjunction with another form or forms, this form may be used in conducting an investigation to determine your suitability or your ability to hold a security clearance, and it may be disclosed to authorized officials making similar, subsequent determinations.

Your Social Security Number (SSN) is needed to keep our records accurate, because other people may have the same name and birth date. Public Law 104-134 (April 26, 1996) asks Federal agencies to use this number to help identify individuals in agency records. Giving us your SSN or any other information is voluntary. However, if you do not give us your SSN or any other information requested, we cannot process your application. Incomplete addresses and ZIP Codes may also slow processing.

**ROUTINE USES:** Any disclosure of this record or information in this record is in accordance with routine uses found in System Notice OPM/GOVT-1, General Personnel Records. This system allows disclosure of information to: training facilities; organizations deciding claims for retirement, insurance, unemployment, or health benefits; officials in litigation or administrative proceedings where the Government is a party; law enforcement agencies concerning a violation of law or regulation; Federal agencies for statistical reports and studies; officials of labor organizations recognized by law in connection with representation of employees; Federal agencies or other sources requesting information for Federal agencies in connection with hiring or retaining, security clearance, security or suitability investigations, classifying jobs, contracting, or issuing licenses, grants, or other benefits; public and private organizations, including news media, which grant or publicize employee recognitions and awards; the Merit Systems Protection Board, the Office of Special Counsel, the Equal Employment Opportunity Commission, the Federal Labor Relations Authority, the National Archives and Records Administration, and Congressional offices in connection with their official functions; prospective non-Federal employers concerning tenure of employment, civil service status, length of service, and the date and nature of action for separation as shown on the SF 50 (or authorized exception) of a specifically identified individual; requesting organizations or individuals concerning the home address and other relevant information on those who might have contracted an illness or been exposed to a health hazard; authorized Federal and non-Federal agencies for use in computer matching; spouses or dependent children asking whether the employee has changed from a self-and-family to a self-only health benefits enrollment; individuals working on a contract, service, grant, cooperative agreement, or job for the Federal government; non-agency members of an agency's performance or other panel; and agency-appointed representatives of employees concerning information issued to the employees about fitness-for-duty or agency-filed disability retirement procedures.

## Public Burden Statement

Public burden reporting for this collection of information is estimated to vary from 5 to 30 minutes with an average of 15 minutes per response, including time for reviewing instructions, searching existing data sources, gathering the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden, to the U.S. Office of Personnel Management, Reports and Forms Manager (3206-0182), Washington, DC 20415-7900. The OMB number, 3206-0182, is valid. OPM may not collect this information, and you are not required to respond, unless this number is displayed.

**Instructions****Read all instructions carefully before completing this form.**

**Anti-Discrimination Notice.** It is illegal to discriminate against any individual (other than an alien not authorized to work in the United States) in hiring, discharging, or recruiting or referring for a fee because of that individual's national origin or citizenship status. It is illegal to discriminate against work-authorized individuals. Employers **CANNOT** specify which document(s) they will accept from an employee. The refusal to hire an individual because the documents presented have a future expiration date may also constitute illegal discrimination. For more information, call the Office of Special Counsel for Immigration Related Unfair Employment Practices at 1-800-255-8155.

**What Is the Purpose of This Form?**

The purpose of this form is to document that each new employee (both citizen and noncitizen) hired after November 6, 1986, is authorized to work in the United States.

**When Should Form I-9 Be Used?**

All employees, citizens, and noncitizens hired after November 6, 1986, and working in the United States must complete Form I-9.

**Filling Out Form I-9****Section 1, Employee**

This part of the form must be completed no later than the time of hire, which is the actual beginning of employment. Providing the Social Security Number is voluntary, except for employees hired by employers participating in the USCIS Electronic Employment Eligibility Verification Program (E-Verify). **The employer is responsible for ensuring that Section 1 is timely and properly completed.**

**Noncitizen Nationals of the United States**

Noncitizen nationals of the United States are persons born in American Samoa, certain former citizens of the former Trust Territory of the Pacific Islands, and certain children of noncitizen nationals born abroad.

**Employers should note** the work authorization expiration date (if any) shown in **Section 1**. For employees who indicate an employment authorization expiration date in **Section 1**, employers are required to reverify employment authorization for employment on or before the date shown. Note that some employees may leave the expiration date blank if they are aliens whose work authorization does not expire (e.g., asylees, refugees, certain citizens of the Federated States of Micronesia or the Republic of the Marshall Islands). For such employees, reverification does not apply unless they choose to present

in **Section 2** evidence of employment authorization that contains an expiration date (e.g., Employment Authorization Document (Form I-766)).

**Preparer/Translator Certification**

The Preparer/Translator Certification must be completed if **Section 1** is prepared by a person other than the employee. A preparer/translator may be used only when the employee is unable to complete **Section 1** on his or her own. However, the employee must still sign **Section 1** personally.

**Section 2, Employer**

For the purpose of completing this form, the term "employer" means all employers including those recruiters and referrers for a fee who are agricultural associations, agricultural employers, or farm labor contractors. Employers must complete **Section 2** by examining evidence of identity and employment authorization within three business days of the date employment begins. However, if an employer hires an individual for less than three business days, **Section 2** must be completed at the time employment begins. Employers cannot specify which document(s) listed on the last page of Form I-9 employees present to establish identity and employment authorization. Employees may present any List A document **OR** a combination of a List B and a List C document.

If an employee is unable to present a required document (or documents), the employee must present an acceptable receipt in lieu of a document listed on the last page of this form. Receipts showing that a person has applied for an initial grant of employment authorization, or for renewal of employment authorization, are not acceptable. Employees must present receipts within three business days of the date employment begins and must present valid replacement documents within 90 days or other specified time.

**Employers must record in Section 2:**

1. Document title;
2. Issuing authority;
3. Document number;
4. Expiration date, if any; and
5. The date employment begins.

Employers must sign and date the certification in **Section 2**. Employees must present original documents. Employers may, but are not required to, photocopy the document(s) presented. If photocopies are made, they must be made for all new hires. Photocopies may only be used for the verification process and must be retained with Form I-9. **Employers are still responsible for completing and retaining Form I-9.**

**For more detailed information, you may refer to the *USCIS Handbook for Employers (Form M-274)*. You may obtain the handbook using the contact information found under the header "USCIS Forms and Information."**

### Section 3, Updating and Reverification

Employers must complete **Section 3** when updating and/or reverifying Form I-9. Employers must reverify employment authorization of their employees on or before the work authorization expiration date recorded in **Section 1** (if any). Employers **CANNOT** specify which document(s) they will accept from an employee.

- A. If an employee's name has changed at the time this form is being updated/reverified, complete Block A.
- B. If an employee is rehired within three years of the date this form was originally completed and the employee is still authorized to be employed on the same basis as previously indicated on this form (updating), complete Block B and the signature block.
- C. If an employee is rehired within three years of the date this form was originally completed and the employee's work authorization has expired **or** if a current employee's work authorization is about to expire (reverification), complete Block B; and:
  - 1. Examine any document that reflects the employee is authorized to work in the United States (see List A or C);
  - 2. Record the document title, document number, and expiration date (if any) in Block C; and
  - 3. Complete the signature block.

Note that for reverification purposes, employers have the option of completing a new Form I-9 instead of completing **Section 3**.

### What Is the Filing Fee?

There is no associated filing fee for completing Form I-9. This form is not filed with USCIS or any government agency. Form I-9 must be retained by the employer and made available for inspection by U.S. Government officials as specified in the Privacy Act Notice below.

### USCIS Forms and Information

To order USCIS forms, you can download them from our website at [www.uscis.gov/forms](http://www.uscis.gov/forms) or call our toll-free number at 1-800-870-3676. You can obtain information about Form I-9 from our website at [www.uscis.gov](http://www.uscis.gov) or by calling 1-888-464-4218.

Information about E-Verify, a free and voluntary program that allows participating employers to electronically verify the employment eligibility of their newly hired employees, can be obtained from our website at [www.uscis.gov/e-verify](http://www.uscis.gov/e-verify) or by calling 1-888-464-4218.

General information on immigration laws, regulations, and procedures can be obtained by telephoning our National Customer Service Center at 1-800-375-5283 or visiting our Internet website at [www.uscis.gov](http://www.uscis.gov).

### Photocopying and Retaining Form I-9

A blank Form I-9 may be reproduced, provided both sides are copied. The Instructions must be available to all employees completing this form. Employers must retain completed Form I-9s for three years after the date of hire or one year after the date employment ends, whichever is later.

Form I-9 may be signed and retained electronically, as authorized in Department of Homeland Security regulations at 8 CFR 274a.2.

### Privacy Act Notice

The authority for collecting this information is the Immigration Reform and Control Act of 1986, Pub. L. 99-603 (8 USC 1324a).

This information is for employers to verify the eligibility of individuals for employment to preclude the unlawful hiring, or recruiting or referring for a fee, of aliens who are not authorized to work in the United States.

This information will be used by employers as a record of their basis for determining eligibility of an employee to work in the United States. The form will be kept by the employer and made available for inspection by authorized officials of the Department of Homeland Security, Department of Labor, and Office of Special Counsel for Immigration-Related Unfair Employment Practices.

Submission of the information required in this form is voluntary. However, an individual may not begin employment unless this form is completed, since employers are subject to civil or criminal penalties if they do not comply with the Immigration Reform and Control Act of 1986.

---

---

### **Paperwork Reduction Act**

An agency may not conduct or sponsor an information collection and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number. The public reporting burden for this collection of information is estimated at 12 minutes per response, including the time for reviewing instructions and completing and submitting the form. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to: U.S. Citizenship and Immigration Services, Regulatory Management Division, 111 Massachusetts Avenue, N.W., 3rd Floor, Suite 3008, Washington, DC 20529-2210. OMB No. 1615-0047. **Do not mail your completed Form I-9 to this address.**

g. I understand that the VA National Rules of Behavior do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

h. I understand that the VA National Rules of Behavior do not supersede any local policies that provide higher levels of protection to VA's information or information systems. The VA National Rules of Behavior provide the minimal rules with which individual users must comply.

**i. I understand that if I refuse to sign this VA National Rules of Behavior as required by VA policy, I will be denied access to VA information and information systems. Any refusal to sign the VA National Rules of Behavior may have an adverse impact on my employment with the Department.**

## 2. SPECIFIC RULES OF BEHAVIOR.

a. I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor and the ISO when the access is no longer needed.

b. I will follow established VA information security and privacy policies and procedures.

c. I will use only devices, systems, software, and data which I am authorized to use, including complying with any software licensing or copyright restrictions. This includes downloads of software offered as free trials, shareware or public domain.

d. I will only use my access for authorized and official duties, and to only access data that is needed in the fulfillment of my duties except as provided for in VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. I also agree that I will not engage in any activities prohibited as stated in section 2c of VA Directive 6001.

e. I will secure VA sensitive information **in all areas** (at work and remotely) and in any form (e.g. digital, paper etc.), to include mobile media and devices that contain sensitive information, and I will follow the mandate that all VA sensitive information must be in a protected environment at all times or it must be encrypted (using FIPS 140-2 approved encryption). If clarification is needed whether or not an environment is adequately protected, I will follow the guidance of the local Chief Information Officer (CIO).

f. I will properly dispose of VA sensitive information, either in hardcopy, softcopy or electronic format, in accordance with VA policy and procedures.

g. I will not attempt to override, circumvent or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized VA staff.

h. I will not attempt to alter the security configuration of government equipment unless authorized. This includes operational, technical, or management security controls.

i. I will protect my verify codes and passwords from unauthorized use and disclosure and ensure I utilize only passwords that meet the VA minimum requirements for the systems that I am authorized to use and are contained in Appendix F of VA Handbook 6500.

j. I will not store any passwords/verify codes in any type of script file or cache on VA systems.

k. I will ensure that I log off or lock any computer or console before walking away and will not allow another user to access that computer or console while I am logged on to it.

l. I will not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any VA electronic communication system.

m. I will not auto-forward e-mail messages to addresses outside the VA network.

n. I will comply with any directions from my supervisors, VA system administrators and information security officers concerning my access to, and use of, VA information and information systems or matters covered by these Rules.

o. I will ensure that any devices that I use to transmit, access, and store VA sensitive information outside of a VA protected environment will use FIPS 140-2 approved encryption (the translation of data into a form that is unintelligible without a deciphering mechanism). This includes laptops, thumb drives, and other removable storage devices and storage media (CDs, DVDs, etc.).

p. I will obtain the approval of appropriate management officials before releasing VA information for public dissemination.,

q. I will not host, set up, administer, or operate any type of Internet server on any VA network or attempt to connect any personal equipment to a VA network unless explicitly authorized **in writing** by my local CIO and I will ensure that all such activity is in compliance with Federal and VA policies.

r. I will not attempt to probe computer systems to exploit system controls or access VA sensitive data for any reason other than in the performance of official duties. Authorized penetration testing must be approved in writing by the VA CIO.

s. I will protect Government property from theft, loss, destruction, or misuse. I will follow VA policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for VA activities.

t. I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by the VA on VA equipment or on computer systems that are connected to any VA network.

u. If authorized, by waiver, to use my own personal equipment, I must use VA approved virus protection software, anti-spyware, and firewall/intrusion detection software and ensure

the software is configured to meet VA configuration requirements. My local CIO will confirm that the system meets VA configuration requirements prior to connection to VA's network.

v. I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee at the time of system problems.

w. I will not disable or degrade software programs used by the VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or to create, store or use VA information.

x. I agree to allow examination by authorized OI&T personnel of any personal IT device [Other Equipment (OE)] that I have been granted permission to use, whether remotely or in any setting to access VA information or information systems or to create, store or use VA information.

y. I agree to have all equipment scanned by the appropriate facility IT Operations Service prior to connecting to the VA network if the equipment has not been connected to the VA network for a period of more than three weeks.

z. I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional required training for the particular systems to which I require access.

aa. I understand that if I must sign a non-VA entity's Rules of Behavior to obtain access to information or information systems controlled by that non-VA entity, I still must comply with my responsibilities under the VA National Rules of Behavior when accessing or using VA information or information systems. However, those Rules of Behavior apply to my access to or use of the non-VA entity's information and information systems as a VA user.

bb. I understand that remote access is allowed from other Federal government computers and systems to VA information systems, subject to the terms of VA and the host Federal agency's policies.

cc. I agree that I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA-approved remote access software and services. I must use VA-provided IT equipment for remote access when possible. I may be permitted to use non-VA IT equipment [Other Equipment (OE)] only if a VA-CIO-approved waiver has been issued and the equipment is configured to follow all VA security policies and requirements. I agree that VA OI&T officials may examine such devices, including an OE device operating under an approved waiver, at any time for proper configuration and unauthorized storage of VA sensitive information.

dd. I agree that I will not have both a VA network connection and any kind of non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by my local CIO.

ee. I agree that I will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and approved in advance by the appropriate VA official (supervisor), and a waiver has been issued by the VA's CIO. I agree that I will not access, transmit or store remotely any VA sensitive information that is not encrypted using VA approved encryption.

ff. I will obtain my VA supervisor's authorization, in writing, prior to transporting, transmitting, accessing, and using VA sensitive information outside of VA's protected environment..

gg. I will ensure that VA sensitive information, in any format, and devices, systems and/or software that contain such information or that I use to access VA sensitive information or information systems are adequately secured in remote locations, e.g., at home and during travel, and agree to periodic VA inspections of the devices, systems or software from which I conduct access from remote locations. I agree that if I work from a remote location pursuant to an approved telework agreement with VA sensitive information that authorized OI&T personnel may periodically inspect the remote location for compliance with required security requirements.

hh. I will protect sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by the VA to protect sensitive data.

ii. I will not store or transport any VA sensitive information on any portable storage media or device unless it is encrypted using VA approved encryption.

jj. I will use VA-provided encryption to encrypt any e-mail, including attachments to the e-mail, that contains VA sensitive information before sending the e-mail. I will not send any e-mail that contains VA sensitive information in an unencrypted form. VA sensitive information includes personally identifiable information and protected health information.

kk. I may be required to acknowledge or sign additional specific or unique rules of behavior in order to access or use specific VA systems. I understand that those specific rules of behavior may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.

# Electronic Questionnaires for Investigations Processing (e-QIP)

## Quick Reference Guide for the Applicant

- System Overview
- Web Browser Requirements
- Getting Started
- Choosing your Golden Questions/Answers
- Entering your Golden Questions/Answers
- Entering your Data
- Displaying your Data
- Listing Expected Attachments
- Certifying your Data

---

**Please note: Applicants can only access the e-QIP system if they have been instructed to do so by an appropriate official at their sponsoring agency. Individuals cannot pre-apply for a security clearance, nor update their pre-existing security questionnaire, unless granted access by an appropriate agency official.**

### System Overview

Welcome to e-QIP, the Electronic Questionnaires for Investigations Processing system. e-QIP is part of an e-government initiative sponsored by the U.S. Office of Personnel Management. e-QIP allows applicants to electronically enter, update, and transmit their personal investigative data over a secure Internet connection to their employing agency for review and approval.

### Web Browser Requirements

**Both Applicant and Agency users must use these settings on their browsers to properly operate e-QIP.**

e-QIP is compatible with Microsoft's Internet Explorer, Netscape Navigator, and Mozilla Firefox. The following specific versions are compatible with e-QIP: (please note any special settings that must be enabled)

If using **Microsoft Internet Explorer (IE)**, you must have version 5.5 or later, with Service Pack 2. Internet Options for IE should be set as follows:

- Select TOOLS
- Select INTERNET OPTIONS
- Select the tab labeled SECURITY
- Select CUSTOM LEVEL
- Check the box to enable ACTIVE SCRIPTING and the OK button to save

To enable TLS 1.0 in IE, on the top menu:

- Select TOOLS
- Select INTERNET OPTIONS
- Select the tab labeled ADVANCED
- Scroll down to the SECURITY section
- Check the box to enable TLS 1.0
- Click the OK button to save

If using **Mozilla Firefox (or Netscape)**, you must have version 0.9.4 or newer. Although security settings may already be defaulted to the proper values, you should verify by doing the following in this order:

- Select "TOOLS"
- Select "OPTIONS"
- Select "ADVANCED"

Select the "ENCRYPTION" tab  
Under Protocols, check the boxes to enable "SSL 3.0" and "TLS 1.0"

**Mozilla Firefox (or Netscape)** users must also verify that they are enabled to use cookies. To do so, go to your browser's toolbar and:

Select "TOOLS"  
Select "OPTIONS"  
Select "PRIVACY"  
Under the "COOKIES" section, ensure that "COOKIES FROM SITES" is checked. e-QIP uses one session cookie.

If using **JAWS** screen-reading software, please note that JAWS requires the use of Internet Explorer, version 5.5 or newer.

### Getting Started

1. Start your internet browser and enter the following URL: <https://www.e-qip.opm.gov/eqip/eQIP>
2. The e-QIP Gateway page will appear. Scroll down and click the button labeled ENTER E-QIP APPLICATION SITE.
3. A "browser checker" utility will automatically run and test your computer. Click the continue button to proceed.
4. A Security Alert box will appear, ending with "Do you want to proceed?" Click the "Yes" button with the mouse, or type <CTRL Y> to continue.
5. The e-QIP Welcome Screen will appear. Enter your Social Security Number in the text entry box, and click the "**Submit**" button to logon to the e-QIP site. You will now answer the (3) default Golden Questions.
6. You must then change the default Golden Questions and Answers to your own personal questions. Be sure to enter three (3) Golden Questions and Golden Answers according to the instructions provided in the Help File on the Golden Question Screen.
7. Complete the investigative form questions and save as instructed.
8. Be sure to Certify/Submit your form when form is complete and all data has been successfully validated.
9. Be sure to print and sign any required release forms before releasing your form for agency review.
10. Make sure to mail your signed signature/release pages to the address provided by your sponsoring agency. Your investigation cannot start until they receive those signed pages

### Choosing Your Golden Questions/Answers

It is **YOUR RESPONSIBILITY** to provide Golden Questions to uniquely identify you. Golden Questions help the e-QIP system verify your identity. By creating a combination of Golden Questions that **ONLY YOU** can possibly know all of the correct answers to, you are assured that no one (including parents, spouses, and close friends) can impersonate you on the e-QIP system. Please carefully consider who else may possibly know the answer to each possible Golden Question you enter. We suggest creating questions concerning different time periods in your life. **PLEASE REMEMBER THAT IT MAY BE 5 YEARS BEFORE YOU RETURN TO THE e-QIP SYSTEM!** Make sure you create questions you can still answer in the distant future.

### Entering Your Golden Questions/Answers

After you have selected your set of Golden Questions/Answers, enter each Question under a "**Question**" header and enter the corresponding Answer under the "**Answer**" header directly under that question. You must provide a non-blank answer for each question you provide, and vice versa. You must provide three Golden Questions.

It is **YOUR RESPONSIBILITY** to protect the answers to your Golden Questions.

Golden Answers are your "password" to the e-QIP system. The text entry fields for Golden Answers are NOT password protected, to allow more accurate entry of your answers. Asterisks automatically mask Golden Answers, but if you choose, you can view your answers by clicking the "*Allow me to see my Golden Answers*" checkbox. Do not allow someone to see your computer screen while your answers are on the screen. If someone acquires your answers, they will be able to logon to the e-QIP system under your identity, allowing them to see and change your personal data.

## Entering Your Data

**NOTE:** Click "Help" from any screen for specific guidance on functions for that screen.

**First Time Data Entry:** Before you begin entering data for the first time, read each instructions document listed on the Read Instructions screen. Indicate that you have read and understand each document by checking the corresponding checkbox. When finished, click the **SUBMIT** button to continue. You must read each document and indicate that you have done so before you may continue.

**Question Navigation:** From any question screen, you may use the Navigation pull-down menu to go to any question, in any order, by selecting the desired section and clicking GO. The Navigation Bar is located in the top right-hand corner of the screen.

**Errors and Warnings:** After clicking **SAVE**, if the system displays the same screen with "**Validation Results**" listed at the top, you must satisfy validation criteria (i.e., there was a problem with your submission that needs to be addressed).

For validation "**Error**" messages, you may correct your data by scrolling to the appropriate field and editing. After making corrections, click the **SAVE** button at the bottom of this page to save your changes.

For validation "**Warning**" messages, you may either provide the requested information or click the **EXPLAIN** button next to the message to explain why the information cannot be supplied. Upon clicking the **EXPLAIN** button you may provide an explanation in the text field or check the box labeled "*I do not know the requested information*". After choosing an action, click the **SAVE** button to save your changes.

For validation "**Error**" and "**Warning**" messages, you may also choose to click the **SAVE/ CONTINUE** button. If you click the **SAVE/ CONTINUE** button, you may advance to the next question screen and correct the information at a later time prior to the final submission of your form.

If you decide to not make any changes, click on the **CANCEL** button to go back to the previous screen.

If you make a mistake and want to start over on a given screen, click on the **RESET THIS SCREEN** button at any time prior to clicking the **SUBMIT** button. This will clear all of your answers on that screen.

When you are finished and ready to proceed, click on the **SAVE** button. Upon clicking the **SAVE** button, your information will be saved.

## Displaying Your Data

When you are ready to display and/or print your personal form information that has been entered into e-QIP, click on the "Display" link located in the upper left hand corner of any e-QIP screen. A new browser window will then appear which will display on the screen all the data that has been entered up to that point. If desired, one can print the displayed data by first selecting "**File**," then "**Print**" from the new browser window.

## Listing Expected Attachments

If desired, you may include additional explanatory information with your signed release forms that will be forwarded to your sponsoring agency. Please ask your sponsoring agency if you are not sure what attachments you are required to provide.

To create a list of "expected attachments", select the **List Expected Attachments** page from the e-QIP Navigation Bar. This screen allows you to create, delete and edit attachments that you will send with your request. This feature does not allow one to upload a document, this is a notation advice to give notice to your sponsoring agency what you will be providing to them by mail or fax.

Then you must mail, drop off, or fax your attachments to your sponsoring/hiring agency, along with your signature forms, per your agency's instructions.

### **Certifying Your Data**

When you have completed all the questions on the form and are ready to submit, click the **Validate, Review, Certify** hyperlink from the Navigation bar, click GO, and follow the instructions.

Certify that the answers you provided on the Questionnaire are correct and accurate. After certification, your answers to the Questionnaire will be locked and unavailable for editing. You should print an official copy of your data for your records and must print a copy of your release forms after you complete certification.

After certification, you must then select ***"Release Request/Transmit to Agency"***