



Commodity Futures Trading Commission Privacy Impact Assessment

System Name: Automated Hiring System, Hosted by Monster Government Solutions

Office: Human Resources Branch

Date: 9/19/2012

1. Overview

The Automated Hiring System (AHS) automates the applicant screening and selection process for CFTC's Human Resources Branch using a third-party internet-based system owned and managed by Monster Government Solutions (MGS or Monster).

When a position becomes available, the CFTC Human Resources (HR) staff posts a vacancy announcement on the job application site owned by Monster. Potential applicants see a job opening listed on CFTC.gov or USAJobs.gov and can click a link to view the full announcement. If interested in applying, an applicant creates an account on the Monster site. The applicant then answers required questions and uploads his or her resume and other requested material, submitting the application when it is complete. The applicant may print a final version in PDF format. When the application period has closed, Monster's systems analyze, filter and sort the applications.

The job applications and Monster's results are accessible to the CFTC HR staff and hiring managers. The HR staff and hiring managers have the ability to rank the applicants, add notes about applicants, and assign and manage each applicant's status, such as "certified" or "meets minimum requirements," "selected," "not selected," or if later contact is made by staff, "failed to reply," or "declined." Applicants may log into the AHS to view the status of their application at any time.

The new system improves the current manual system by efficiently and quickly analyzing, sorting and filtering applications based on an applicant's answers to preset questions, allowing a faster determination of which applicants meet minimum criteria. AHS allows quick and accurate communication between HR staff and hiring managers about applicants and their status in the selection process, while also providing applicants with prompt notification of status. In addition, AHS enables CFTC to post its own vacancy announcements, which reduces the cost and time currently involved in arranging for another Federal agency to post the announcements. Moreover, for applicants who provide voluntary demographic information, AHS captures race, ethnicity, sex, age, disability and other similar information needed by the CFTC to evaluate the effectiveness of recruitment and outreach efforts.

AHS significantly improves the privacy and security of job application-related information. This secure automated system will minimize the risk of loss or accidental disclosure of information that is inherent in the current manual, paper-based system.

2. Data Collected and Stored Within the System

2.1. What personally identifiable information (PII) will be collected, used, disseminated or maintained in the system?

For individuals who create an account on Monster and/or apply for a vacancy, MGS stores and processes name, personal and business contact information, employment history and work experiences, veteran status, professional resume, and account credentials. Specifically, the system includes the following:

1. PII Categories	2. Is collected, processed, disseminated, stored and/ accessed by this system or project	3. CFTC Employees	4. Members of the Public	5. Other (e.g. contractors, other government employees)
Name (for purposes other than contacting federal employees)	X	X	X	X
Date of Birth				
Social Security Number*	X	X		X
Tax Identification Number (TIN)				
Photographic Identifiers				
Driver's License				
Mother's Maiden Name				
Vehicle Identifiers				
Personal Mailing Address	X	X	X	X
Personal E-Mail Address	X	X	X	X
Personal Phone Number	X	X	X	X
Medical Records Number				
Medical Notes or some other Health Information (specifically for AHS, disability or accommodation information)	X	X	X	X
Financial Account Information				
Legal Documents				
Device Identifiers				
Web Uniform Resource Locator(s)				
Education Records	X	X	X	X
Military Status	X	X	X	X
Employment Status	X	X	X	X
Foreign Activities				
Other for AHS:				
- citizenship	X	X	X	X
- employment history/work experience	X	X	X	X
- qualifications/competencies, test results and similar information	X	X	X	X

- comments from HR staff and hiring managers	X	X	X	X
- status of application, e.g., meets minimum criteria, selected, not selected	X	X	X	X

**Required only for current or former federal employees, as part of the SF-50, Notification of Personnel Action, and for former service members, DD-214 form, Certificate of Release or Discharge from Active Duty.*

Those who register on MGS and/or apply for a position (collectively, “applicants”) may also voluntarily provide demographic information, including race, ethnicity, sex, mental or physical disability or accommodation needs. Applicants may provide additional data, including possibly sensitive PII such as social security number, in documents they upload in their application or in free-text responses.

2.2. What will be the sources of the information in the system?

CFTC hiring managers, HR staff and job applicants will be the sources of the information in the system.

2.3. Why will the information be collected, used, disseminated or maintained?

The purpose of the collection and use of the information is to streamline and improve management of the applicant evaluation, selection and hiring processes.

2.4. How will the information be collected and used by the Commission?

MGS is a tool that utilizes the public Internet to solicit and manage applications from job seekers. Applicants will be able to view vacancy announcements and input information into the Monster tool to apply for a position. The MGS tool will analyze, filter and sort applications and allow HR staff and hiring managers to view applications, add notes and update the status of applicants. Applicants will be able to view the status of their application.

The vacancy announcement, information submitted by the applicant, and information provided by CFTC HR staff and hiring managers will be stored and managed on Monster’s information technology systems, accessible by different users through user-created accounts.

2.5. Is the system using technologies in ways that the CFTC has not previously employed (e.g., monitoring software)?

No, AHS is not using technologies in way that the CFTC has not previously employed. This type of internet-based tool is common to CFTC systems. Technologies being used to configure the Monster interface conform to the CFTC’s Office of Data and Technology (ODT) standards.

2.6. What specific legal authorities authorize the collection of the information?

The legal authorities for the collection include 5 U.S.C. 1302, 5 U.S.C. 301, and Commodity Exchange Act, 7 U.S.C. § 2(a)(2) et seq. When requested of current and former federal employees and service members on the SF-50 and DD-214 forms,

solicitation of the Social Security Number is also authorized by Executive Order 9397, which allows Federal agencies to use this number to help identify individuals in agency records. Additional authorities are identified in the applicable government-wide System of Records Notices, OPM/GOVT-5, Recruiting, Examining, and Placement Records, and for any voluntarily provided demographic information, OPM/GOVT-7, Applicant Race, Sex, National Origin, and Disability Status Records.

3. Data and Records Retention

3.1. How will the information in this system be managed throughout its lifecycle? For what period of time will data collected by this system be maintained and in what form will the data be retained?

For retention and disposition purposes, information in the system will be maintained as case files, so all information related to a vacancy announcement will be deleted at the same time. The records will be maintained and dispositioned in accordance with records disposition schedules for the records involved, as approved by the National Archives and Records Administration.

3.2. What are the plans for destruction and/or disposition of the information?

The case files within the Automated Hiring System will be deleted 3 years after HRB has closed the files, in accordance with General Records Schedule 1, Item 33p and the additional guidance specified in OPM's "Delegated Examining Operations Handbook: A Guide for Federal Agency Examining Offices."

4. Access to and Sharing of the Data

4.1. Who will have access to the information in the system (internal and external parties), and with whom will the data be shared? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

CFTC hiring managers and HR staff will have access to the information contained in the AHS.

When the system requires maintenance or an applicant uses the "Help" function within the MGS, employees of Monster may access to information in the system. Monster has represented in contracts that it will maintain the confidentiality of the information in the system and that Federal security standards apply to all data being held by Monster for the CFTC. Monster employees must pass a background check that includes examination of criminal conviction records, credit bureau records, and verification of previous employment. The CFTC's Financial Management Branch, the Chief Privacy Officer and Chief Information Security Officer have reviewed the contract documentation for compliance with applicable law.

4.2. If the data will be shared outside the Commission's network, how will the data be transferred or shared?

The data contained in the system will not be transferred outside the Monster-owned system, although hiring managers or HR staff may print or download application material for purposes of applicant selection and hiring.

Limited information in an application may be shared with an individual outside of the CFTC if the hiring manager calls a job applicant's references to verify information in the application or to seek additional information about the applicant. Applicants are notified that, "All the information you provide may be verified by a review of the work experience and/or education as shown on your application form, by checking references and through other means, such as the interview process."

The information also may be shared in accordance with the applicable government-wide System of Records Notices, OPM/GOVT-5, Recruiting, Examining, and Placement Records, and for demographic information, OPM/GOVT-7, Applicant Race, Sex, National Origin, and Disability Status Records.

4.3. Do other systems share the information or have access to the information in this system? If yes, explain who will be responsible for protecting the privacy rights of the individuals affected by the interface (e.g., System Administrators, System Developers, System Managers)?

As represented by Monster, the owner of the site, no other information technology systems will electronically share the information or have access to the information in AHS.

5. Notice, Consent and Access for Individuals

5.1. What notice will be provided to individuals about the collection, use, sharing and other processing of their personal data?

Notice is provided to applicants through a Privacy Policy & Privacy Act Statement available on the Monster site during the application process and through this Privacy Impact Assessment.

5.2. What opportunities will exist for an individual to decline to provide information or to consent to particular uses of the information? If opportunities exist, how will this notice be given to the individual and how will an individual grant consent?

Failure to provide the requested information through the MGS system will delay processing of an application, and failure to submit required information before a vacancy announcement closes will result in an application not being considered.

Applicants may apply for a position without using the MGS system by contacting CFTC's HR staff directly:

Commodity Futures Trading Commission
Human Resources Branch
Three Lafayette Centre
1155 21st St., NW
Washington DC 20581

Phone 202-418-5003
Email: employment@cftc.gov

5.3. What procedures will exist to allow individuals to gain access to their information and request amendment/correction, and how will individuals be notified of these procedures?

At any point while the vacancy is open, applicants have the ability to update or change the information they have saved or uploaded within MGS. Applicants are notified of both of these policies during the application process.

Once a vacancy announcement has closed, applicants seeking access to records about themselves, or seeking amendment of records about themselves should contact CFTC's HR staff, at the address noted above, or address a written inquiry to the Office of General Counsel, Paralegal Specialist, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581, telephone (202) 418-5011.

6. Maintenance of Controls

6.1. What controls will be in place to prevent the misuse of the information by those having authorized access and to prevent unauthorized access, use or disclosure of the information?

The information is protected from misuse and unauthorized access through various administrative, technical and physical security measures. Technical security measures within CFTC include restrictions on computer access to authorized individuals, required use of strong passwords that are frequently changed, use of encryption for certain data types and transfers, and regular review of security procedures and best practices to enhance security. Physical measures include restrictions on building access to authorized individuals and maintenance of records in lockable offices and filing cabinets.

Monster has represented in contract documentation that it follows all Federal information security requirements, including the Federal Information Security Management Act (FISMA) and certain National Institute of Standards and Technology (NIST) publications. Monster has represented that data in transit and at rest is encrypted, including data in transit during the application submission process, and application information residing on Monster systems.

6.2. While the information is retained in the system, what will the requirements be for determining if the information is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

At any point while the vacancy is open, applicants may determine if information they have provided is accurate, relevant, timely and complete. They have the ability to view, update or change the information they have saved or uploaded within the AHS.

The information contained in the system will be protected from alteration and deletion through administrative, technical and physical controls as noted above. Additionally, Monster reviews its audit records on a regular basis for indications of inappropriate or unusual activity in the AHS.

6.3. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No.

6.4 Are all IT security requirements and procedures required by Federal law being followed to ensure that information is appropriately secured?

The CFTC follows, and Monster has represented through contract documents that it follows, all applicable FISMA requirements to ensure that the information found in AHS is appropriately secured.

MGS, if breached, would result in a moderate potential impact on individuals or organizations, as categorized under the Federal Information Processing Standards (FIPS) 199.

6.5. Describe the privacy training provided to users either generally or specifically relevant to the program or system.

All CFTC personnel are subject to CFTC agency-wide policies and procedures for safeguarding PII. They receive annual privacy and security training and annually sign a CFTC "Information Technology Rules of Behavior." Many staff receive additional training, for example, each year new supervisors receive additional training, and in June 2012, the Human Resources Branch received training specifically focused on human resources information.

In addition, all Monster employees who work on the AHS must attend annual security awareness and training, and sign and acknowledge that they have read and agree to abide by Monster's "rules of behavior," e.g., maintaining confidentiality of information in the system.

7. Privacy Act

7.1. Will the data in the system be retrieved by a personal identifier in the normal course of business? If yes, explain. If not, can it be retrieved by a personal identifier?

Yes. Information will be retrieved by name.

7.2 Is the system covered by an existing Privacy Act System of Records Notice ("SORN")? Provide the name of the system and its SORN number, if applicable.

Yes, government-wide System of Records Notice OPM/GOVT-5, Recruiting, Examining, and Placement Records. Voluntarily provided demographic information is included in government-wide System of Records Notice OPM/GOVT-7, Applicant Race, Sex, National Origin, and Disability Status Records.

8. Privacy Policy

8.1. Confirm that the collection, use and disclosure of the information in this system have been reviewed to ensure consistency with the CFTC's Privacy Policy on www.cftc.gov.

The privacy policy on www.cftc.gov is not applicable. Instead, a privacy policy specifically designed for the job application system is available on the Monster-hosted job application site: [CFTC Job Application Privacy Policy & Privacy Act Statement](#).

9. Privacy Risks and Mitigation

9.1. What privacy risks are associated with the collection, use, dissemination and maintenance of the data? How have those risks been mitigated?

The risk of job application data being disclosed or accessed without authorization has been mitigated by use of strong security measures in the transmission and storage of the data. For example, to mitigate the risk from external forces, the PII data is encrypted in transit in accordance with FIPS 140-2. Further, the PII is encrypted at rest using Advanced Encryption Standard (AES) 256 encryption.

Also, Monster utilizes an intrusion detection system (IDS) to monitor inbound and outbound network connections for all network activity. The IDS monitors for unusual or unauthorized activities or conditions and flags any events for review. Unusual or unauthorized activities or conditions include the presence of malware, malicious code, spyware, adware, the unauthorized export of data and the signaling to an external information system. The IDS system retains logs for a minimum of 6 months and all potential security incidents are investigated.

Privacy risks are further minimized by collecting only that data necessary for the job application, selection and hiring process. Social security numbers are not specifically solicited in the job application form, and are only required on SF-50 and DD-214 forms of current and former federal employees and service members.