CRS Insights

OPM Data Breach: Personnel Security Background Investigation Data

Michelle D. Christensen, Analyst in Government Organization and Management (mchristensen@crs.loc.gov, 7-0764)

July 24, 2015 (IN10327)

In a July 9, 2015, news release on the cyber-intrusions of its systems, OPM "concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases." OPM's background investigation databases contain sensitive personal information on individuals (including congressional staff) who have undergone a personnel security background investigation as part of the security clearance process. This sensitive personal information may include financial and credit data, details on alcohol or illegal drug use, names of foreign contacts, or mental health information.

OPM's systems also contain information on individuals without security clearances, but who have undergone a background investigation for other reasons. For example, OPM conducts background investigations on individuals whose positions involve policymaking, law enforcement, or other responsibilities that demand a great deal of "public trust," even if the positions do not require access to classified materials.

According to OPM, the breach includes data from 19.7 million current, former, and prospective employees and contractors who applied for a background investigation after 2000. Additionally, the breach includes personally identifiable information of 1.8 million non-applicants, which OPM states are primarily "spouses or co-habitants of applicants." OPM also confirmed that "the usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen," and that some of the records compromised by the breach include fingerprints.

The investigation into the OPM breach is ongoing. This CRS Insight provides information on the types of data that may be collected in a typical personnel security background investigation and is not an official statement of the data that was compromised in the OPM breach.

What Information Is Collected on OPM's Background Investigation Forms?

The information collected will depend on the applicant's position and the type of background investigation required. OPM uses three standard forms for background investigations: SF-85, SF-85P, or SF-86 form. The forms are typically submitted electronically using OPM's Electronic Questionnaires for Investigations Processing (e-QIP) system. OPM had suspended use of e-QIP "for security enhancements," but re-enabled the system on July 23, 2015.

Data Collected for Non-Sensitive Positions

The eight-page SF-85 is required for applicants to non-sensitive positions (e.g., positions that do not require a security clearance) who require physical access to government facilities and who are in positions with a "low risk" to cause damage to the federal government or national security. The responsibilities of these positions are limited and there is little opportunity to use such positions for personal gain. For this reason, the information collected is relatively limited in scope and includes

- full name, aliases, and SSN;
- citizenship information;
- employment information and addresses for the past five years; and
- information on use or possession of illegal drugs (including marijuana) in the previous year.

Data Collected for "Positions of Public Trust"

The 11-page SF-85P is required for applicants in "Positions of Public Trust," (i.e., positions that do not involve access to classified information, but that demand a "significant degree of public trust" due to the level of policymaking or other responsibilities). These positions may involve a "significant risk for causing damage [to the federal government] or realizing personal gain." In addition to the information listed above, the SF-85P requires

- identifying information (e.g., height, weight, eye and hair color);
- military service information;
- employment information and addresses for the past seven years;
- schools, if any, attended during the past seven years;
- name, address, and telephone number of three personal references and immediate family members;
- criminal arrests and/or convictions for the past seven years (excluding incidents prior to the applicant's 16th birthday or traffic fines under $150);
- financial information, including bankruptcies during the past seven years and any delinquent financial obligations;
- foreign travel during the past seven years; and
- information on use or possession of illegal drugs (including marijuana) in the previous year and any illegal purchase, sale, or transport of drugs in the previous seven years.

Data Collected for Security Clearances and Other National Security Positions

The 127-page SF-86 form is required for applicants to national security sensitive positions, which includes (but is not limited to) positions that require a security clearance. In addition to the information listed above, the SF-86 requires

- employment information and home addresses for the past 10 years;
- schools attended for the past 10 years, including a reference at each school attended;
- personal information (including SSN) for current spouse or cohabitant;
- foreign contacts, travels, and/or activities;
- associations with individuals or groups dedicated to terrorism or the violent overthrow of the U.S. government;
- details on applicant's "psychological and emotional health," including, with certain exceptions, details on treatments during the past seven years;
- additional information on criminal activities, including convictions or charges involving firearms or explosives;
- alcohol use in the past seven years that has negatively impacted the applicant's work, personal relationships, finances, or resulted in "intervention by law enforcement/public safety personnel";
- use, possession, or other involvement with illegal drugs (including marijuana) in the past seven years or at any time while holding a clearance;
- details on the applicant's financial condition and civil court actions; and
- improper use of information technology systems.

What Other Records Are Contained in OPM's Personnel Security Background Investigation Files?

OPM's systems also include information gathered by investigators during the background investigation process, such as summaries of interviews with the applicant's family members, co-workers, friends, and neighbors. Additionally, investigators may run credit checks, pull civil and criminal court records, and run checks of state and federal agency records to verify information that the applicant provided on the application.

According to OPM's most recent Privacy Act Notice, personnel investigation records may also include information provided by other agencies, such as

- Internal Revenue Service income tax returns;
- prior security clearance investigative records; and
- clearance adjudicative records, including polygraph results, if applicable.

It is unclear from OPM's news release if these types of investigative records were compromised in the breach.