THE PRESIDIO

Privacy Act of 1974; System of Records

AGENCY: The Presidio Trust

ACTION: Notice of a new System of Records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Presidio Trust is issuing a public notice of its intent to establish a communications solution, system of records. PRESIDIO TRUST/Department of Public Safety-01, Genasys Emergency Management (GEM) Mass Communications Software Solution.

DATES: This system of records is effective upon publication. New routine uses will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may send comments, identified by PRESIDIO TRUST/Department of Public Safety-01, via email to the interim Privacy Officer, within Presidio Trust's Department of Administration, Luke Donohue, LDonohue@presidiotrust.gov. or via U.S. Mail 1750 Lincoln Blvd. San Francisco, CA, 94129

FOR FURTHER INFORMATION CONTACT: Director of Administration, Luke Donohue, LDonohue@presidiotrust.gov, or 415-561-5300.

SUPPLEMENTARY INFORMATION: The Presidio Trust, Department of Public Safety, is establishing PRESIDIO TRUST/Department of Public Safety 01, Genasys Emergency Management (GEM) Mass Communications Software Solution, systems of records. Genasys® provides multi-channel mass communication delivered via text, email, and voice to key stakeholders in an emergency, and to select target audiences: Presidio Trust Staff; Presidio Park Residents and Commercial Tenants; and Presidio Park Visitors, Neighborhood Organizations, Partners, and Hospitality. Presidio Trust staff information is maintained as standard employee data. Genasys messaging is sent only to agency-issued email accounts and mobile devices. Presidio Resident and Commercial Tenant information is maintained in an existing leasing database; Genasys messaging is sent to email accounts and mobile devices provided by the recipient. Presidio Resident and Commercial Tenants are offered an opportunity to opt-out with every message. Presidio Park visitors and others self-opt into the system. These individuals provide their own email and/or mobile numbers and may opt-out at any time. Personal contact information will be used to contact and alert participants to public safety and emergencies that occur in the park. To the extent permitted by law, information may be shared with Federal, state, local, and tribal agencies, and organizations as authorized and compatible with the purpose of this system, or when proper and necessary, consistent with the routine uses set forth in this system of records notice.

System Name and Number: PRESIDIO TRUST/Department of Public Safety 01, Genasys Emergency Management (GEM) Mass Communications Software Solution

Security Classification: Unclassified.

System Location: Presidio Trust, Department of Public Safety, 1750 Lincoln Boulevard, San Francisco, CA 94129. Genasys Inc., 16262 W. Bernardo Drive, San Diego, CA 92127.

System Manager(s): Department of Public Safety, 1750 Lincoln Blvd. San Francisco, CA 94129, Safety@presidiotrust.gov

Authority for Maintenance of the System: 5 U.S.C. 552a.

Purpose(s) of the System: The primary purpose of this system is to provide a notification delivered via

text, email, or voice in the event of an emergency situation.

Categories of Individuals Covered by the System: Individuals covered by the system include Presidio Trust Staff, Presidio Park Residents and Commercial Tenants, and Presidio Park Visitors, Neighborhood Organizations, Partners, and Hospitality.

Categories of Records in the System: The system contains records which include first name, last name, personal cell phone number, and/or email address.

Record Source Categories: Records in Genasys are obtained from multiple sources. Employee and Tenant information exists in current, existing databases such as EOPF, and is maintained as standard employee data. Staff are not provided with an opt out option for emergency messaging. Tenant information exists in an existing Yardi database; Genasys messaging is sent to email accounts and mobile devices provided by the recipient. Presidio Resident and Commercial Tenants are offered an opportunity to opt-out with every message. Presidio Park visitors and others self-opt into the system. Individuals provide their own email and/or mobile numbers and may opt-out at any time. This audience remains in the system until they opt-out.

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside the Department of Interior as a routine use pursuant to 5 U.S.C. 552a(b)(3) may be made to:

(1) The appropriate Federal, State, local or foreign agency responsible for obtaining information relevant for investigating, prosecuting, enforcing, or implementing a statue, rule, regulation, or order when Presidio Trust becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

(2) The U.S. Department of Justice or in a proceeding before a court or adjudicative body when:

(a) The United States, the Presidio Trust, a component of the Presidio Trust, or, when represented by the government, an employee of the Presidio Trust is a party to litigation or anticipated litigation or has an interest in such litigation, and

(b) The Presidio Trust determines that the disclosure is relevant and necessary to the litigation and is compatible with the purpose for which the records were compiled.

(3) To a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

(4) To appropriate agencies, entities, and persons when:

(a) The Presidio Trust suspects or has confirmed that there has been a breach of the system of records

(b) The Presidio Trust has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, The Presidio Trust (including its information systems, programs, and operations), the Federal Government, or national security.

(c) The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with The Presidio Trusts efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(5) To another Federal agency or Federal entity, when the Presidio Trust determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in:

(a) Responding to a suspected or confirmed breach.

(b) Preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national or national security, resulting from a suspected or confirmed breach.

(6) To Contractors when the contractor is working on a contract, service, job, or other activity for the

Agency and who have a need to have access to the information in performance of their duties or activities for the Agency. Recipients will be required to comply with the requirements of the Privacy Act of 1974 as provided in 5 U.S.C. 552a(m).

Policies and Practices for Storage of Records: Electronic records are contained in computers, and on secured servers located in a controlled facility with limited access and managed by Genasys. When transmitting highly confidential information, Genasys uses industry standard Secure Sockets Layer (SSL) encryption technology for secure data transmission. Access is restricted through physical controls and system security practices.

Policies and Practices for Retrieval of Records: Records in this system can be retrieved by either querying within the application or generating a report. The information may be retrieved by various fields including name, personal email address, home address, or phone number.

Policies and Practices for Retention and Disposal of Records: Residential and Commercial tenant PII is updated as new tenants are manually registered. PII is retained until a tenant leaves, or opts-out of the system, whichever comes first. Visitors may opt-in at their discretion and opt-out at a time of their choosing. Employee PII is retained until an employee separate from Presidio Trust. All data held on a Genasys database will be scrubbed 30 days after a contract between Presidio Trust and Genasys Inc. is terminated**.**

Administrative, Technical, and Physical Safeguards: All records contained in this system are safeguarded with applicable security and privacy rules and policies. Genasys meets ISO 27001 Security and Network compliance and ISO 22320 Emergency Management requirements, and all cloud procedures meet NIST 500-299 recommendations. The software is hosted on Amazon AWS cloud SSAW-18, company is SOC1 & SOC2 certified, 27001 certified, and maintains Cloud Security Genasys emergency Management (GEM) System of Records Notice (SORN) Alliance (CSA) STAR Attestation. Their certifications indicate that the services, processes, and facilities have been comprehensively reviewed and meet stringent security standards. Genasys uses industry-standard Secure Sockets Layer (SSL) encryption technology for secure data transmission. Genasys has a comprehensive Disaster and Recovery Plan defining the procedures to recover backups in the event of an IT systems' critical failure. Genasys is protected by industry-standard security measures that include two factor network authentication, enterprise-class firewalls, network-based Intrusion Detection Software (IDS),

network vulnerability scanning tools, and anti-virus software with real-time definition updates. Genasys' network is firewall enabled with a three-layer architecture that controls HTTPS access, IP address control access, two-way client server TLS certificates, and the maximum number of connections allowed per IP.

Genasys does not access, share, or distribute any customer data. All employees with access to privacy data must review and sign a security access policy document. Access authorization is controlled by the HR Manager, IT Manager, and CEO; Access to the data is limited to a needs-only basis. The Presidio Trust has limited access to the Genasys System to only Department of Public Safety and Emergency Communications staff. Application activities are logged at multiple levels to provide a full audit of system activity for monitoring and troubleshooting. Audit logs, execution logs, and information to generate KPIs of the system behavior are stored by Genasys. Audits comply with applicable industry regulations and are hardened to prevent tampering. Daily system scans are conducted by Genasys and can be accessed by Trust staff holding administrative access. The solution incorporates anti-virus protection to guard against malicious upload and distribution of unacceptable content. Genasys maintains detailed logs on: Database maintenance activities; System Administrator; General operator/administrator access; and Application configuration changes. Genasys customer data is logically partitioned and encrypted at rest.

Record Access Procedures: An individual requesting access to their records should send a written inquiry to the applicable System Manager identified above. Presidio Trust forms and instructions for submitting a Privacy Act request may be obtained from the Presidio Trust Privacy Act Requests website at https://www.Presidio Trust.gov/privacy/privacy-act requests. The request must include a general description of the records sought and the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requestor's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked “PRIVACY ACT REQUEST FOR ACCESS” on both the envelope and letter. A request for access must meet the requirements of 43 CFR 2.238.

Contesting Record Procedures: An individual requesting amendment of their records should send a written request to the applicable System Manager as identified above. Presidio Trust instructions for submitting a request for amendment of records are available on the Presidio Trust Privacy Act Requests website at https://www.Presidio Trust.gov/privacy/privacy act-requests. The request must clearly identify the records for which amendment is being sought, the reasons for requesting the amendment, and the proposed amendment to the record. The request must include the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requestor's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked “PRIVACY ACT REQUEST FOR AMENDMENT” on both the envelope and letter. A request for amendment must meet the requirements of 43 CFR 2.246.

Notification Procedures: An individual requesting notification of the existence of records containing their personally identifying information, should send a written inquiry to the applicable System Manager as identified above. Presidio Trust instructions for submitting a request for notification are available on the Presidio Trust Privacy Act Requests website at https://www.Presidio Trust.gov/privacy/privacy-act-requests. The request must include a general description of the records and the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requestor's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28

U.S.C. 1746. Requests submitted by mail must be clearly marked “PRIVACY ACT INQUIRY” on both the envelope and letter. A request for notification must meet the requirements of 43 CFR 2.235.

Exemptions Promulgated for the System: No.

History: No.

Luke Donohue,
Director of Administration.

[FR Doc. 2024-04007 Filed: 2/26/2024 8:45 am; Publication Date: 2/27/2024]