From: ICE Privacy-General Mailbox
Sent: 18 Apr 2018 17:35:14 +0000
To: (b)(6);
Subject: FW: Safeguarding Sensitive Personally Identifiable Information
Attachments: Fw: Safeguarding Sensitive Personally Identifiable Information

Will do. Please attached email.

(b)(6);
Privacy Compliance Specialist
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct: (202) 732-(b)(6)
Main: (202) 732-(b)(6);

From: (b)(6);
Sent: Wednesday, April 18, 2018 1:27 PM
To: ICE Privacy-General Mailbox <(b)(6); (b)(7)(C)
Subject: Re: Safeguarding Sensitive Personally Identifiable Information

thanks, can you forward me the email and assign to me in POTS? I'll handle this one.

From: ICE Privacy-General Mailbox
Sent: Wednesday, April 18, 2018 1:26:37 PM
To: (b)(6);
Subject: FW: Safeguarding Sensitive Personally Identifiable Information

This just came in from (b)(6); from ERO. I am going to put it in POTS, and in the tracker.

(b)(6);
Privacy Compliance Specialist
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct: (202) 732-(b)(6)
Main: (202) 732-(b)(6)

From: (b)(6); (b)(7)(C)
Sent: Wednesday, April 18, 2018 1:14 PM
To: ICE Privacy-General Mailbox <(b)(6); (b)(7)(C)
Subject: Fw: Safeguarding Sensitive Personally Identifiable Information

Good afternoon,

I'm an acting Unit Chief at Domestic Operations and we had a question about privacy issues and PII or SPII as it relates to our High Profile Removal notifications and other communication. These notifications are typically shared with government entities within DHS to provide final notification that a high profile removal is imminent and the operation plan includes specifics of the removal operation. The broadcast below from Mr. Albence raised some questions about to whom these notices are sent and what we can have in the Subject line, etc... I'm happy to provide more background on the topic if you need to or if you need any additional information.

Thanks,

From: ERO Taskings
Sent: Tuesday, April 17, 2018 10:20 AM
Subject: Safeguarding Sensitive Personally Identifiable Information

The following message is sent on behalf of Matthew T. Albence, Executive Associate Director for Enforcement and Removal Operations:

To: **All ERO Personnel**

Subject: **Safeguarding Sensitive Personally Identifiable Information**

The purpose of this message is to remind all ERO employees of the importance of protecting Sensitive Personally Identifiable Information (Sensitive PII).

In our mission to identify, arrest, and remove aliens that are a risk to public safety, ERO collects Sensitive PII from aliens, citizens, legal residents and visitors, such as Names and Alien Registration Numbers. We are obligated by law and DHS policy to protect this information to prevent identity theft or other adverse consequences of a privacy incident or misuse of Sensitive PII data.

The DHS Performance and Learning Management System (PALMS) offers a mandatory course titled, “Privacy at DHS: Protecting Personal Information.” This course is designed to raise employee awareness of the importance of maintaining privacy in the workplace and sets out clear methods for safeguarding Sensitive PII and for reporting any breach or loss of sensitive data.

All ERO employees are required to complete the PALMS course annually by **September 30, 2018**. Visit the PALMS home page at (b)(7)(E) In the interim, please take this opportunity to review the attached DHS factsheet on how to properly collect, use, share and dispose of Sensitive PII.

A few reminders:

- PII should not be included in the subject lines of email.
- When you send Sensitive PII in email to users with a need to know AND to a non-dhs.gov account, DHS policy requires ICE employees and contractors to send Sensitive PII in an encrypted or password protected attachment.
- When you send electronic files in the mail, DHS policy recommends any removable media (e.g., CD, DVD) is password protected and it must be sent using a tracking number or return receipt.

To obtain more detailed requirements and recommendations on the safe handling of PII, download the "Handbook for Safeguarding Sensitive PII" at www.dhs.gov/privacy or contact the ICE Office of Information Governance and Privacy at (202) 732 (b)(6);

From: (b)(6); (b)(7)(C)
Sent: 18 Apr 2018 17:14:23 +0000
To: ICE Privacy-General Mailbox
Subject: Fw: Safeguarding Sensitive Personally Identifiable Information
Attachments: How to Safeguard Sensitive PII.PDF

Good afternoon,

I'm an acting Unit Chief at Domestic Operations and we had a question about privacy issues and PII or SPII as it relates to our High Profile Removal notifications and other communication. These notifications are typically shared with government entities within DHS to provide final notification that a high profile removal is imminent and the operation plan includes specifics of the removal operation. The broadcast below from Mr. Albence raised some questions about to whom these notices are sent and what we can have in the Subject line, etc... I'm happy to provide more background on the topic if you need to or if you need any additional information.

Thanks,

From: ERO Taskings
Sent: Tuesday, April 17, 2018 10:20 AM
Subject: Safeguarding Sensitive Personally Identifiable Information

The following message is sent on behalf of Matthew T. Albence, Executive Associate Director for Enforcement and Removal Operations:

To: **All ERO Personnel**

Subject: **Safeguarding Sensitive Personally Identifiable Information**

The purpose of this message is to remind all ERO employees of the importance of protecting Sensitive Personally Identifiable Information (Sensitive PII).

In our mission to identify, arrest, and remove aliens that are a risk to public safety, ERO collects Sensitive PII from aliens, citizens, legal residents and visitors, such as Names and Alien Registration Numbers. We are obligated by law and DHS policy to protect this information to prevent identity theft or other adverse consequences of a privacy incident or misuse of Sensitive PII data.

The DHS Performance and Learning Management System (PALMS) offers a mandatory course titled, "Privacy at DHS: Protecting Personal Information." This course is designed to raise employee awareness of the importance of maintaining privacy in the workplace

and sets out clear methods for safeguarding Sensitive PII and for reporting any breach or loss of sensitive data.

All ERO employees are required to complete the PALMS course annually by **September 30, 2018**. Visit the PALMS home page at (b)(7)(E) In the interim, please take this opportunity to review the attached DHS factsheet on how to properly collect, use, share and dispose of Sensitive PII.

A few reminders:

- PII should not be included in the subject lines of email.
- When you send Sensitive PII in email to users with a need to know AND to a non-dhs.gov account, DHS policy requires ICE employees and contractors to send Sensitive PII in an encrypted or password protected attachment.
- When you send electronic files in the mail, DHS policy recommends any removable media (e.g., CD, DVD) is password protected and it must be sent using a tracking number or return receipt.

To obtain more detailed requirements and recommendations on the safe handling of PII, download the "Handbook for Safeguarding Sensitive PII" at www.dhs.gov/privacy or contact the ICE Office of Information Governance and Privacy at (202) 732-(b)(6);