UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

UNITED STATES OF AMERICA v. MICHAEL SCHEUER	Case No. 6:25-cr-5-JSS-DCI

UNITED STATES' SENTENCING MEMORANDUM

The United States of America submits this sentencing memorandum in support of a 70-month term of incarceration in this case.

PRELIMINARY STATEMENT

On January 29, 2025, the Court adjudicated the defendant guilty of (1) computer fraud, in violation of 18 U.S.C. § 1030(a)(5)(A) and (2) aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1), following his guilty plea.

This case centers on a series of cyber intrusions and attacks directed at Company A by the defendant, a former employee. The cyber intrusions initially targeted menus at restaurants operated by Company A. They ranged from altering menu fonts, backgrounds, and their underlying configuration files, to manipulating pricing and item descriptions, to altering allergen information. These changes were designed to effect discord, as Company A mobilized resources to combat the intrusions, bring its programs back online, and ultimately remediate the damage, including to its systems. Standing apart was the defendant's alteration of allergen information—the defendant manipulated allergen information on "allergy-friendly" menus to indicate that food

items were safe for customers with particular allergies when they were not in fact safe, thus jeopardizing the health (and potentially the lives) of restaurant customers.

Later, the cyber-attacks became more personal, as the defendant launched serial denial-of-service attacks against fourteen individual employees, some of whom were involved in his termination. These denial-of-service attacks involved commandeering the usernames for these employees' work accounts and simulating thousands of incorrect login attempts to thus lock them out. All of the intrusions implicated high levels of sophistication, as they involved the use of distinctive virtual private networks (VPNs), multiple virtual computers (i.e., computers within a computer), and layers of encryption. These tools were not only used to facilitate the intrusions but to conceal the defendant's conduct.

What is clear is that the defendant's conduct was increasingly escalatory during the course of the attacks. The intrusions began following his termination in June 2024. And they ceased when the FBI executed a search warrant of his residence and seized his computers on September 23, 2024. Things later came to a head when the defendant was seen late at night outside the home of one of the denial-of-service victims. He was then charged by complaint (ECF 1) and arrested the next day, (ECF 6). But for his arrest, the defendant's conduct would have continued to trend more and more dangerous.

What is also clear, however, is that the defendant's actions were attributable—at least in part—to a mental health episode. The government does not dispute that the evidence, including mental health records, electronic communications, and interviews

and testimony, tends to show that the defendant's mental health decline rapidly intensified following his termination from Company A. The government also does not dispute that the defendant is sincere in his commitment to seeking and persisting in mental health treatment going forward.

The United States requests a sentence of 70 months' incarceration. This sentence—depending on the guideline range ultimately adopted by the Court—is likely to be a downward variance. As set forth below and with respect to each 3553(a) factor, the government believes this sentence strikes an appropriate balance among the competing factors and is sufficient, but not greater than necessary, to achieve the purposes of sentencing.

BACKGROUND

Whereas the Presentence Investigation Report ("PSR") includes a thorough and detailed recitation of the offense conduct, (ECF 58, ¶¶11-48), the United States submits the following overview of the cyber intrusions (subsection A, *infra*) and additional details and context for the second intrusion, which included the manipulation of allergen information (subsection B, *infra*).

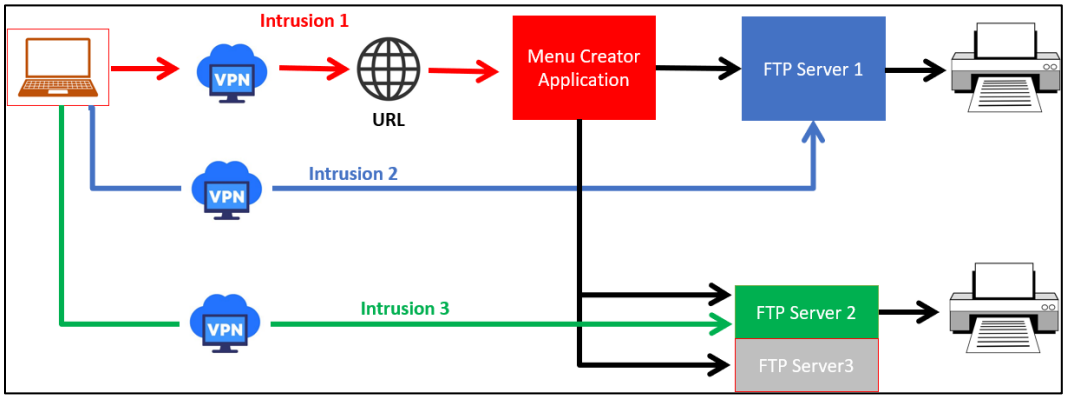
A. Overview of cyber intrusions

As noted, the cyber intrusions and attacks began following the defendant's June 2024 termination, and stopped in late September 2024. The intrusions fall into four categories and progressed as follows:

1. Intrusion 1 – accessing Company A's menu design program and altering font configuration files and menu images and backgrounds, (ECF 58, ¶¶12-19);

2. Intrusion 2 – accessing a Company B server and making alterations to, among other things, allergen information in handheld menus, (*id.*, ¶¶20-25);
3. Intrusion 3 – accessing a Company A server and making changes to, among other things, QR codes on large, display-style menus, (*id.*, ¶¶26-28); and
4. Denial-of-service attacks – launching denial-of-service attacks against fourteen Company A employees, including by using employee usernames and running a script to effect serial unsuccessful login attempts of their work accounts and to thereby cause the accounts to shutdown, (*id.*, ¶¶29-36).

Intrusions 1 – 3, are further reflected below:



(ECF 1, p.5).

B. Manipulation of allergen information

Intrusion 2 was particularly egregious because it involved the alteration of allergen information within Company A menus and thus the conscious (or, in the least, reckless) risk of death or serious bodily injury to customers of Company A.

Company A maintains "allergy-friendly" menus at its restaurants. Within these menus, food items are typically followed by a brief description, then a list of allergies

for which each food item is safe. As part of Intrusion 2, the defendant added allergies under food items to reflect that the item was safe for a customer with a particular allergy (e.g., a peanut allergy), when it was not in fact safe and could be deadly:

DINNER

ALLERGY-FRIENDLY MENU

ENTRÉES

STEAKHOUSE CUTS*

Served with choice of one (1) Side and one (1) Sauce

8-oz Beef Tenderloin Medallions 42
For Gluten/Wheat, Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, Sesame, and Soy Allergies

6-oz Top Sirloin Steak 32
For Gluten/Wheat, Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, Sesame, and Soy Allergies

8-oz Filet Mignon 41
For Gluten/Wheat, Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, Sesame, and Soy Allergies

14-oz Dry-aged Pork Bone-In Rib Chop 34
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

10-oz New York Strip 38
For Gluten/Wheat, Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, Sesame, and Soy Allergies

12-oz Roasted Prime Rib 39
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

SAUCES

*Enhance your experience with a Flight of all five (5) Sauces*** 6

Signature Steakhouse 51
For Gluten/Wheat, Egg, Milk, Peanut/Tree Nut, Sesame, Shellfish, and Soy Allergies

Béarnaise
For Gluten/Wheat, Peanut/Tree Nut, Sesame, Shellfish, and Soy Allergies

Red Wine
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Whipped Horseradish Cream
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Salsa Verde
For Gluten/Wheat, Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, Sesame, and Soy Allergies

SIDES

Mashed Potatoes
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Red Wine-glazed Mushrooms
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Au Gratin Potatoes
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Seasonal Vegetables
For Gluten/Wheat, Egg, Fish/Shellfish, Milk, Sesame, and Soy Allergies

Macaroni & Cheese
For Egg, Fish/Shellfish, Peanut/Tree Nut, and Sesame Allergies

Charred Asparagus
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Creamed Spinach
White Wine Mornay Sauce
For Egg, Fish/Shellfish, Peanut/Tree Nut, and Sesame Allergies

Cream of Corn
For Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Add Cheddar Cheese, Scallions, or Bacon 4
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

ENHANCEMENTS**

Shrimp 12
For Gluten/Wheat, Egg, Fish, Peanut/Tree Nut, Sesame, and Soy Allergies

Oscar 15
For Gluten/Wheat, Peanut/Tree Nut, Sesame, and Soy Allergies

Fish of the Day*
Risotto-style Orzo, White Wine Cream Sauce, Butternut Squash Purée 31
For Egg, Milk, Peanut/Tree Nut, Sesame, and Shellfish Allergies

Pan-seared Chicken
Mozzarella and Prosciutto-stuffed, Mashed Potatoes, Seasonal Vegetables, Chardonnay-Mustard Sauce 28
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Vegetable "Wellington"
Mushroom Duxelles and Fire-roasted Artichokes wrapped in Puff Pastry, Romesco, Brussels Sprouts 27
For Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, and Sesame Allergies

Alterations Made to Menu

- **Vegetable "Wellington"**
  - Added friendly for: Tree Nut allergy
- **Fish of the Day**
  - Added friendly for: Milk allergy
- **Seasonal Vegetables**
  - Added friendly for: Milk allergy
  - Removed Peanut/Tree Nut allergy
- **8-oz Filet Mignon**
  - Changed steak size from 6 to 8-oz

(**Exhibit 1** hereto).

ALLERGY-FRIENDLY BRUNCH MENU

Guests must speak to a [redacted] about their Allergy-Friendly request. While we take steps to help mitigate cross-contact, we cannot guarantee that any item is completely free of allergens. Our Allergy-Friendly recipes may use highly refined oils, such as soybean oil, and/or ingredients that are processed in facilities that also process allergens. It is ultimately our Guests' discretion to make an informed choice based upon their individual dietary needs. For more information about Allergy-Friendly requests, ask to speak with [redacted] upon arrival at the location.

APPETIZERS

Shrimp Cocktail
Jumbo Shrimp, Key West Cocktail Sauce, Tropical Slaw, and Citrus 16
For Gluten/Wheat, Fish, Milk, Peanut/Tree Nut, and Sesame Allergies

Tropical Fruit
Chef-inspired offering served with Açai Pudding 14
For Gluten/Wheat, Egg, Fish/Shellfish, Milk, Peanut, Sesame, and Soy Allergies

Conch Fritters
Served with Key Lime Mustard 15
For Peanut/Tree Nut and Sesame Allergies
Substitute Savory Hushpuppies with Honey Butter 12
For Fish, Milk, Peanut/Tree Nut, and Sesame Allergies

ENTRÉES

Southernmost Buttermilk Chicken
Served with choice of Scrambled Eggs, Olivia's Breakfast Potatoes, Biscuit, and Southern Gravy 26
or
Mashed Potatoes, Southern Gravy, Biscuit, and Seasonal Vegetables 23
For Fish, Milk, Peanut/Tree Nut, and Sesame Allergies

Crab Cake-Eggs Benedict*
Poached Eggs and Crab Cakes on a Buttermilk Biscuit with Key Lime Hollandaise served with Olivia's Breakfast Potatoes 26
For Fish, Peanut/Tree Nut, and Sesame Allergies

Buttermilk Pancakes
Served with Scrambled Eggs and choice of Bacon or Sausage 16
For Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Seared Salmon Salad*
Mixed Greens, Quinoa, Avocado, Mandarin Orange, Edamame, and Key Lime Vinaigrette 17
For Gluten/Wheat, Egg, Milk, Peanut/Tree Nut, Sesame, and Shellfish Allergies

Olivia's Breakfast*
Two Eggs-Any Style and Olivia's Breakfast Potatoes served with Allergy-Friendly Toast and choice of Bacon or Sausage
For Gluten/Wheat, Fish, Milk, Peanut/Tree Nut, Sesame, and Soy Allergies

Blackened Fish Tacos*
Mahi Mahi with Tropical Slaw, Avocado Crema, Cilantro, Lime, and French Fries 21
For Peanut/Tree Nut, Sesame, and Shellfish Allergies

Banana Bread French Toast
Topped with a Bahamian Banana-Rum Syrup, Crème Anglaise, and Whipped Cream served with choice of Bacon or Sausage 19
For Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Sombrero Beach Omelet
Ham, Green Peppers, Onions, and Cheddar with Sour Cream and Pico de Gallo served with Olivia's Breakfast Potatoes and Allergy-Friendly Toast 17
For Gluten/Wheat, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Caesar Salad with Chicken
Grilled Chicken and Chopped Romaine tossed with Parmesan, House-made Croutons, and Caesar Dressing 15
For Fish/Shellfish, Peanut/Tree Nut, and Sesame Allergies
Substitute Shrimp 17
For Fish, Peanut/Tree Nut, and Sesame Allergies

Papa's Hash
Potatoes, Spinach, Plant-based Sausage, Plant-based Frittata, and Tomatoes 16
For Gluten/Wheat, Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, and Sesame Allergies

Bacon Cheeseburger*
Cheddar, Crispy Onions, Avocado, and Bacon Jam with House-made Key West Ketchup and Aioli 25
For Fish/Shellfish, Peanut/Tree Nut, and Sesame Allergies

SIDES

Bacon 5.5
For Gluten/Wheat, Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, Sesame, and Soy Allergies

Sausage 5.5
For Gluten/Wheat, Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, Sesame, and Soy Allergies

Olivia's Breakfast Potatoes 5.5
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Grits 5.5
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, Sesame, and Soy Allergies

Buttermilk Biscuit 5.5
For Egg, Fish/Shellfish, Peanut/Tree Nut, and Sesame Allergies

An 18% gratuity is added for parties of 6 or more.
[redacted] proudly purchases cage-free eggs.
*This item is cooked to Guest preference and/or may contain raw or undercooked ingredients. Consuming raw or undercooked meats, poultry, seafood, shellfish, or eggs may increase your risk of foodborne illness.
**Not included in the Dining Plan.

[redacted]

Alterations Made to Menu

- **Southernmost Buttermilk Chicken**
  - Added friendly for: Milk allergy
  - Altered price - $3
- **Olivia's Breakfast**
  - Added friendly for: Milk allergy
  - Removed price
- **Sides**
  - Removed asterisks

(**Exhibit 2** hereto).

Allergy-Friendly Menu

[redacted]

Entrées

ANGUS BEEF BURGER*
with Lettuce and Tomato on an Allergy-Friendly Bun served with choice of French Fries, Potato Tots, or Fresh Fruit 23
For Gluten/Wheat, Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, Sesame, and Soy Allergies

IMPOSSIBLE™ BURGER
Plant-based Patty, Plant-based Mayonnaise, and Seasonal Vegetable Relish on an Allergy-Friendly Bun served with choice of French Fries, Potato Tots, or Fresh Fruit 23
For Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, and Sesame Allergies

BEACHES & CREAM GRILLED CHEESE
with Creamy Tomato Soup 18
Add Bacon or Ham 5 each
Tomato Soup may be substituted with French Fries, Potato Tots, or Fresh Fruit
For Fish/Shellfish, Peanut/Tree Nut, and Sesame Allergies

FRENCH DIP SANDWICH
Thinly Sliced Roast Beef, Swiss Cheese, and Au Jus on an Allergy-Friendly Bun served with choice of French Fries, Potato Tots, or Fresh Fruit 22
For Gluten/Wheat, Egg, Milk, Peanut/Tree Nut, Sesame, and Soy Allergies

REUBEN SANDWICH
Corned Beef, Sauerkraut, Swiss Cheese, and Thousand Island Dressing on Marbled Rye Bread served with choice of French Fries, Potato Tots, or Fresh Fruit 20
For Fish/Shellfish, Peanut/Tree Nut, and Sesame Allergies

CHEDDAR-BACON-RANCH CHICKEN SANDWICH
with Sauteed Onion, Lettuce, and Tomato on an Allergy-Friendly Bun served with choice of French Fries, Potato Tots, or Fresh Fruit 21
For Gluten/Wheat, Fish/Shellfish, and Peanut/Tree Nut Allergies

BOWL OF CHILI
Topped with Cheese and Green Onions 10
For Gluten/Wheat, Egg, Peanut/Tree Nut, and Sesame Allergies

Sweet Endings

COOKIE FRIES WITH DIPPING SAUCE
Cookie Fries with Assorted Dips 8.5
For Egg, Fish/Shellfish, Milk, Peanut/Tree Nut, Sesame, and Soy Allergies

BROWNIE À LA MODE
Allergy-Friendly Brownie, Hot Fudge, and Vanilla Ice Cream topped with Whipped Cream, Chocolate Sprinkles, and a Cherry 9.25
For Gluten/Wheat, Peanut, and Sesame Allergies

OLD-FASHIONED SUNDAE
Soy-based Frozen Dessert with choice of one of the following toppings: Marshmallow, Strawberry, Pineapple, Peanut Butter, or Chocolate Syrup topped with Toasted Almonds and a Cherry
Two-Scoops 9.25 Three-Scoops 10
Extra Toppings 1 each
For Gluten/Wheat, Egg, Fish/Shellfish, Sesame, and Milk Allergies

NO WAY JOSE
A Peanut Butter and Hot Fudge delight featuring Chocolate and Vanilla Ice Cream, Peanut Butter and Chocolate Morsels, Whipped Cream, and a Cherry 13.5
For Gluten/Wheat, Fish/Shellfish, Sesame, and Tree Nut Allergies

An 18% gratuity is added for parties of 6 or more.
*This item is cooked to Guest preference and/or may contain raw or undercooked ingredients. Consuming raw or undercooked meats, poultry, seafood, shellfish, or eggs may increase your risk of foodborne illness.

Alterations Made to Menu

- **Brownie A La Mode**
  - Added friendly for: Peanut allergy
  - Removed Fish/Shellfish allergy

(**Exhibit 3** hereto).[1]

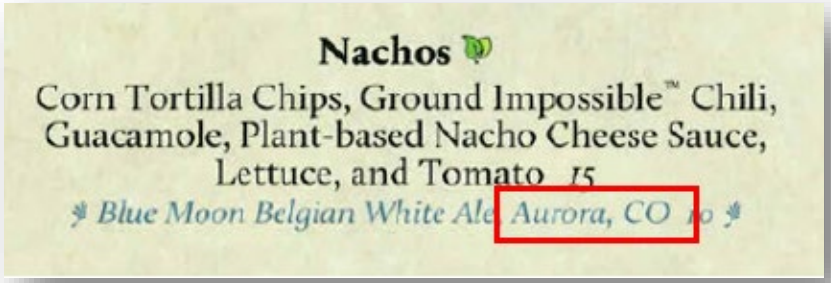
[1] The defense's sentencing memorandum misstates that both "fish/shellfish" and "peanut" were added to the brownie item. (ECF 60, p.5). But there is no "fish/shellfish" on the altered menu; instead, this allergy removed and replaced with "peanut." In doing so, the defendant indicated that this item was safe for individuals—including the children likely to order this item—with peanut allergies.

This also undoes the defense's point that adding a "shellfish" allergy to a dessert item would be "obvious" or "hypocritical to the menu item itself." Indeed, before its removal, "shellfish" was listed, and all of the other dessert items list this allergy.

Additionally, the timing of these alterations suggests it was designed to inflict maximum reputational harm to Company A. Specifically, these changes began during a string of media coverage related to litigation involving the death of a customer with nut and dairy allergies at a Company A restaurant. In other words, the alterations were designed to cause similar customer injury and to then exploit that injury for maximum reputational harm to Company A.

In addition to the allergen-related alterations, other menu changes were particularly malevolent. For example, in certain menus, wine and beer regions were altered to reflect locations of recent mass shootings:

Alteration
Changed "Willamette Valley" to "Apalachee High"



Alteration
Changed "Golden, CO" to "Aurora, CO"

(**Exhibits 4** and **5** hereto).

To be sure, many of the allergen alterations were discreet. They were also accompanied by other innocuous or less consequential changes, including for example changes to pricing or item descriptions (e.g., steak size). But this does not detract from the significance of the changes. Instead, the discreet way in which these changes were made was likely by design, specifically to avoid detection.

MEMORANDUM

At the upcoming sentencing hearing, the United States will request that the Court adopt the guideline calculation in the PSR, overrule the defendant's objections to same, and balance the 3553(a) factors to impose a sentence of 70-months' incarceration.

I. The Defendant's Objections to the PSR Should Be Overruled.[2]

A. Reckless risk of death or serious injury

The enhancement for conscious or reckless risk of serious bodily injury or death under USSG §2B1.1(b)(16) is properly applied. To the extent there remains an objection to this enhancement, it should be overruled.

Under §2B1.1(b)(16), a two-level enhancement is applied if the offense involved "the conscious or reckless risk of death or serious bodily injury." The Eleventh Circuit has "noted that the guideline 'focuses on the defendant's disregard of risk, rather than on the result.'" *United States v. Henderson*, 893 F.3d 1338, 1351 (11th Cir. 2018) (*United States v. Moran*, 778 F.3d 942, 977 (11th Cir. 2015)). "The Government need not show

[2] The government also incorporates its letter in response to the defense's objections (**Exhibit 6** hereto), which was not attached to the PSR.

actual injury to any particular victim." *Id.* "Rather, the question is whether the defendant placed the victim at such a risk." *United States v. Achille*, 277 F. App'x 875, 877-78 (11th Cir. 2008) (quoting *United States v. Snyder*, 291 F.3d 1291, 1294-95 (11th Cir.2002)).

Here, manipulating allergen information in Company A menus endangered customers suffering from those allergies. Simply put, a real-world outcome could have been for a customer suffering from—for example—a peanut allergy to order a menu item believing it to be safe and, having then consumed that item, to suffer severe bodily injury, including anaphylaxis and death. Creating this risk was by design and thus done consciously, or in the least recklessly. Further, as noted, the timing of the changes suggests it was specifically designed to exploit customer injury to instill maximum reputational harm to Company A.

It is not a defense that the defendant believed the changes might be noticed by Company A through "additional layers of proofing" and would thus not make it to customers. (ECF 58, p.82). As noted, this enhancement "focuses on the defendant's disregard of risk, rather than on the result." *Henderson*, 893 F.3d at 1351 (quotation omitted). Further, the changes were discreet and comparatively limited, thus indicating their aim was to avoid detection. There are also no facts in the PSR or the record to show what additional proofing would have been applied, how that proofing operated, and thus the likelihood of catching the alterations. Third, reliance on the hope that these potential deadly alterations would have been caught after the proofing process is in the least "reckless" and thus still covered by §2B1.1(b)(16). *See Henderson*,

893 F.3d at 1351-52 (applying enhancement for faulty administrative entries in medical records that "could have delayed or influenced patient care"; "The Government did not need to show actual evidence of death or serious bodily injury"); *United States v. Cannon*, 41 F.3d 1462, 1467 (11th Cir. 1995) (enhancement applies even though substandard aircraft parts never failed or caused any harm; further unclear whether those parts were ever even installed).

B. Use of special skill

The adjustment for the use of a special skill in the commission or concealment of the offense under USSG §3B1.3 is appropriately applied. And the defense's objection should be overruled.

"Special skill" includes skills "not possessed by members of the general public." USSG §3B1.3, comment. (n.4). The Sentencing Commission lists examples of persons with special skills as "pilots, lawyers, doctors, accountants, chemists, and demolition experts." *Id.* This list, however, is not exhaustive. And courts readily find that advanced computer skills, or computer skills beyond those of the general public, count as "special skills" under §3B1.3. *See, e.g.*, *United States v. Campa*, 529 F.3d 980, 1017 (11th Cir. 2008) ("Skills in … computer technology are legitimate skills that Guerrero turned to criminal purposes." (citing *United States v. Prochner*, 417 F.3d 54, 62 (1st Cir. 2005) (computer skills))); *see also United States v. Reichert*, 747 F.3d 445, 455 (6th Cir. 2014) (applying enhancement where defendant's "skill with computer hardware and specialized game console components was substantially more difficult to acquire than the mere familiarity with desktop publishing").

Here, the defendant's computer skills were well beyond those of the general public. The defendant employed his specialized skills to hide his conduct through distinctive VPNs, virtual computers,[3] and layers of encryption. He further used his specialized skills to manipulate configuration files, background imaging, and QR codes. Specifically with respect to the denial-of-service attacks, the defendant developed a script to simulate thousands of serial login attempts and to effectively render work accounts unusable. These are legitimate computer skills that were used for criminal purposes. And these are not skills possessed by members of the general public.

II. The Section 3553(a) Factors Favor the Sentence Requested by the United States.

The 3553(a) factors favor a 70-month term of incarceration. This sentence reflects a downward variance from the guideline range. Namely, it includes a 46-month term on Count 1, and the required 24-month term on Count 2. The requested sentence strikes a balance between facts favoring a meaningful term of incarceration and those tempering such concerns.

A. Nature and circumstances of the offense

On the one hand, considerations related to the offense conduct militate in favor of a meaningful term of incarceration. As discussed above, the offenses involved a series

[3] The defense does not appear to formally object to the "sophisticated means" enhancement under §2B1.1(b)(10)(C). (ECF 58, pp.81-82). But the defense's commentary on this enhancement conflates VPNs with "virtual computers," which are two different things. Additionally, while the use of VPNs by businesses is not uncommon, the distinctive VPN used here was.

of complex and sustained cyber-attacks directed at Company A. These attacks were designed to create chaos and to conceal their source and extent. As reflected in the loss amount, (ECF 58, ¶50), they ultimately required substantial investigation and remediation by Company A. The attacks progressed through phases—when one option became unviable (due to, for example, password resets), the defendant pivoted to a new attack. Ultimately, in September 2024, the attacks became more personal, as he used employee information to launch thousands of denial-of-service attacks to lockout these employees from their enterprise accounts.

The attacks were also dangerous. A real-world consequence of manipulating the allergen information as part of Intrusion 2 could have been the serious bodily injury or death of unsuspecting customers of Company A. Indeed, their timing indicates this was by design and to maximize reputational harm to Company A. And at the time of the defendant's arrest, his actions were trending more and more dangerous.

On the other hand, considerations of the offense conduct are mitigated—at least in part—by the defendant's compromised mental health. The government does not dispute this was likely *a* driver of the defendant's behavior and helps to explain his increasingly erratic and confrontational behavior. The government further does not dispute the sincerity and commitment of the defendant to seek and persist in treatment.

Another mitigating consideration is the defendant's acceptance of responsibility. While three levels are already accounted for in the guideline range, the government does not dispute that the defendant's acceptance exceeded that of a typical defendant entering into a plea agreement. Following his arrest, the defendant promptly

accepted responsibility, expressed substantial remorse, and assisted with the government's investigation.

B. History and characteristics of the defendant

Considerations of the history and characteristics of the defendant also favor the downward variance (to 70-months) requested by the government. As reflected in the PSR, the defendant has no criminal history. He is also the father of three young children and is the sole breadwinner for his family.

C. Just punishment, adequate deterrence, respect for the law, and protection of the public

Here again, the 3553(a)(2) factors tilt in favor of a meaningful sentence yet are mitigated by competing considerations.

Deterrence and respect for the law. The defendant's conduct *during* the course of the attacks tilts toward the need for incarceration to promote deterrence and respect for the law. During this time period and as discussed above, the defendant's conduct was calculated, sustained, and dangerous. He was undeterred by the hurdles he encountered when conducting the intrusions; he simply pivoted to new and different attacks. His communications with law enforcement also reflect a brazenness and disregard for the rule of law—when he learned of a search warrant executed on his Google account, he emailed the FBI agent directly and, among other things, demanded they speed up their investigation. (*See* ECF 23-6 ("Also Tim please add your [Company A] contact, this is taking to[o] long")).

Nevertheless, the defendant's conduct *after* his arrest, tilts in the other direction.

As noted, once removed from his escalatory environment, the defendant promptly took responsibility for his actions, expressed remorse, and sought to remedy the damage he caused. The government does not dispute that, following a term of incarceration and continued treatment, the risk of recidivism can be minimized.

Protection of the public. The same considerations apply—*during* the course of the offense conduct, the defendant was a danger to both the public as well as certain of the individual victims. The United States and the Court were mindful of these concerns during the defendant's detention hearing; though the defendant requested release to seek in-patient mental health treatment, safety concerns precluded pretrial release.[4]

Yet *after* his arrest and time in pretrial detention, concerns regarding danger trend in the other direction. The government is hopeful these concerns will ultimately be alleviated. Though a term of incarceration is needed to separate the defendant,

[4] In the defense's sentencing memorandum, the defense asserts that the basis for his pretrial detention was a "ransom note" email received by the mother of one of the defendant's denial-of-service victims (DPR); coincidentally, this same note was found on the defendant's desktop, next to a folder titled "dox," which contained, among other things, the mother's personal information. (ECF 60, pp.8-9). The defense asserts that this email was not in fact sent by the defendant and that he was detained pretrial because of the "Government's mistake."

This is wrong for several reasons. First, the primary reason for the defendant's pretrial detention was because he had showed up late at night at the home of one of his denial-of-service victims. No doubt, these safety concerns foreclosed pretrial release. Second, the government has always been amendable to a framework for the defendant to receive in-patient treatment, while ensuring the safety of his victims. The defense was unable to propose a viable framework during the detention hearing, and the Court thus rejected the defense's request. Third, as a factual matter, the government's witness acknowledged that a larger phishing scam had used versions of the note. Finally, despite claiming there was a "mistake" at the detention hearing, the defense has not once asked the Court to revisit detention. That is because, as noted, the above-noted safety concerns were the driver of pretrial detention.

temporally, from his state of mind at the time of the attacks.

III. Additional considerations regarding Victims

Attached to the PSR are victim statements from DP and AG, both of whom were victims of the defendant's denial-of-service attacks and involved in his termination. (ECF 58, pp.32-36). It is the United States' understanding that DP intends to address the Court at the sentencing hearing. *See* Fed. R. Crim. P. 32(i)(4)(B); *see also* 18 U.S.C. § 3771(a)(4).

Additionally, the United States also requests that, as part of a special condition of supervised release, the Court preclude the defendant from contacting any of the victims of the offense conduct or otherwise identified in this case, including: Company A,[5] Company B,[6] DP, AG, DH, TS, MB, JV, PW, PT, AM, CS, JK, GH, MS, SP, and DPR.[7] *See* 18 U.S.C. § 3563(b)(6) (discretionary condition available to prohibit defendant from associating with "specified persons").

CONCLUSION

Wherefore, the United States respectfully requests that this Court sentence the defendant to a term of incarceration of 70 months and impose the above-requested special condition of supervised release.

[5] Identified in paragraph 11 of the PSR.

[6] Identified in paragraph 12 of the PSR.

[7] Identified by their initials in paragraph 31 of the PSR.

Dated: April 18, 2025

Respectfully submitted,

GREGORY W. KEHOE
United States Attorney

By: /s/ Robert D. Sowell
Robert D. Sowell
Assistant United States Attorney
FBN 113615
Office of the United States Attorney
400 W. Washington St., Ste. 3100
Orlando, FL 32801
407-648-7500
Robert.sowell@usdoj.gov