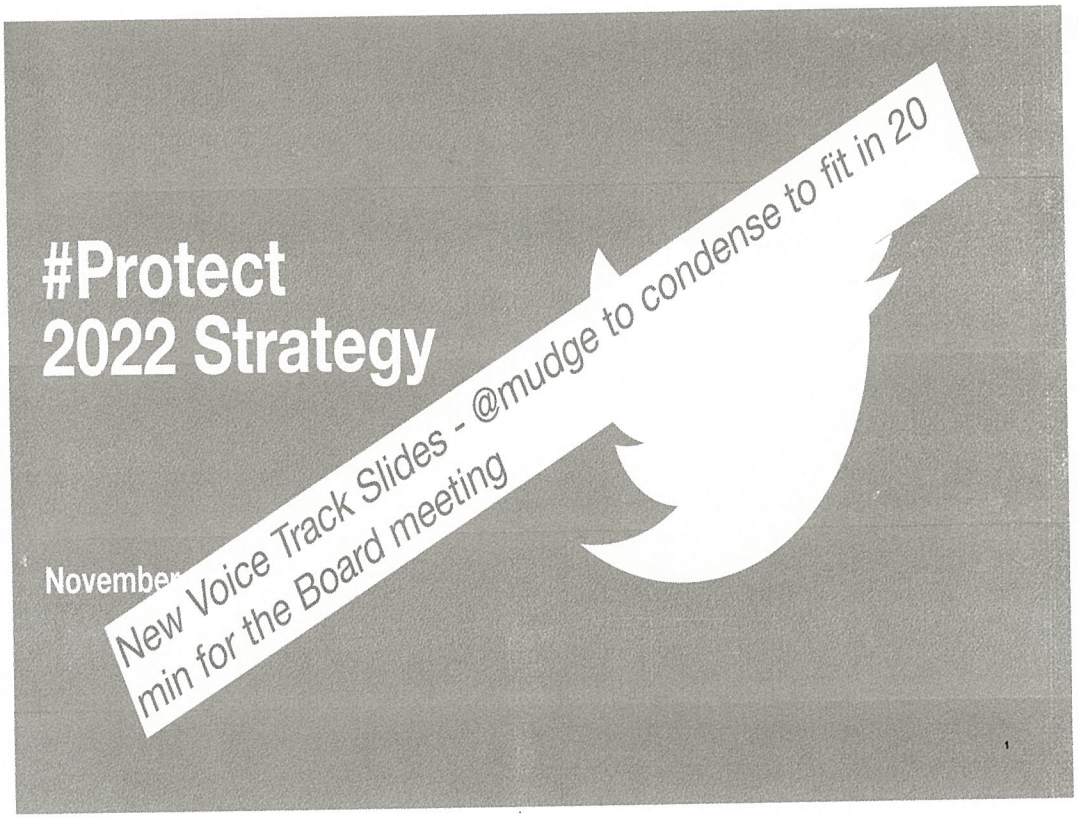
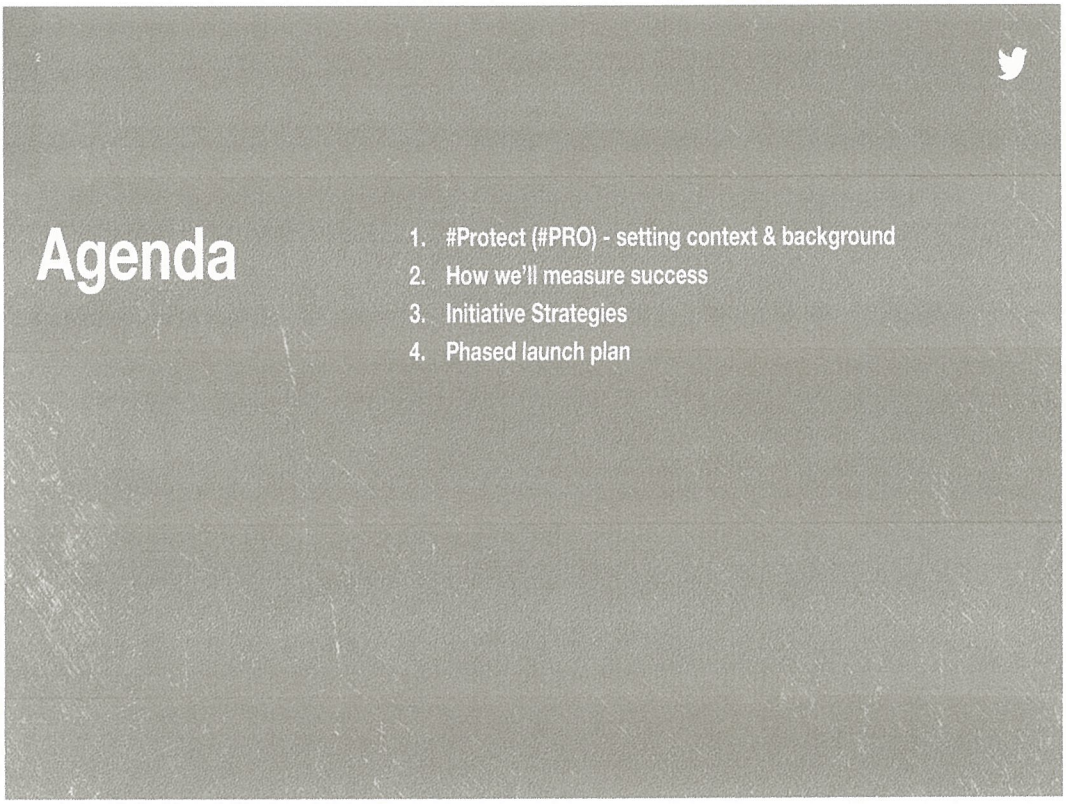


#PRO Strategy Doc (3-page doc for the Board)


Agenda
1. #Protect (#PRO) - setting context & background
2. How we'll measure success
3. Initiative Strategies
4. Phased launch plan

30 sec

#PRO

The #Protect (#PRO) Objective's mission is to
protect Twitter and it's Customers
from people who could cause harm to us or
do harm to others through our platform.

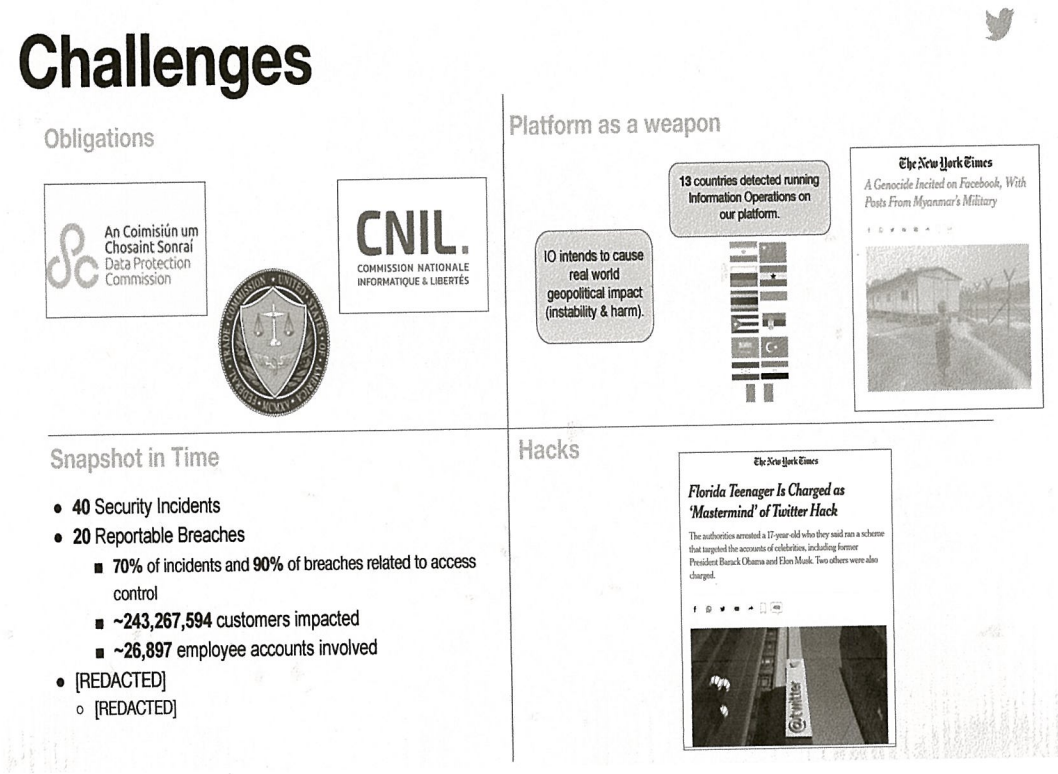
[1 min for this slide]
And that's the mission: protect Twitter and its Customers against the people who would cause us harm or do harm to others through our platform.

That's the "why" and the difference in "focus" of Protect-objective in 2-ish slides.

Into the "what and how"

Why we needed to create #PRO

Setting context and background



[3 min for this slide]
For a broader audience each of these could be a slide - walking through the issue, the threat, and who/what we are protecting ourselves and our Customers from and how well (or poorly) we are positioned to do so.

Here, we can go through these in 90 seconds.

Top Left
We are getting closer to the final FTC consent - an agreement that will last for 20 years covering everything we do with data as a company. Brought on by misuse of data from a lack of data protection and privacy controls. Other regulatory bodies are focusing on us… and more will be coming.

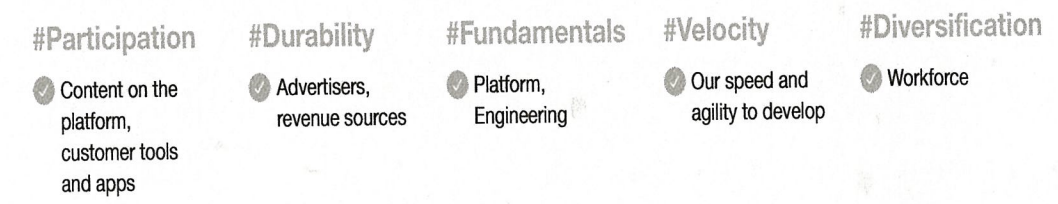
Top Right
We have disclosed 13 Countries running Information Operations on our Platform (that we know of!). ~~There are people intent on abusing the public conversation and FaceBook and Myanmar are the cautionary tale.~~ Facebook admitted they failed to stop their platform being used to cause a genocide. The Myanmar military assumed false personas and incited murders, rapes, and the largest forced human migration in recent history.

Bottom Right
The big twitter code-red hack wasn't sophisticated. It hit only one of several areas in which we have very large exposure. My understanding is that it delayed hiring for over a month and more than 6k person hours spent in the immediate wake of the event.

Bottom left - these are signals that we're sitting on top of other code reds.
There's no finger pointing. There are always tradeoffs and people make the best decisions they can. But a strategy of reacting and trusting that we are excellent scrambling in a crisis (we are) can't be our strategy going forward.

Let's look at the Twitter Objectives and how Protect's focus addresses challenges on this slide in a complimentary fashion to the other objectives. And in a way we aren't focusing currently.

Existing Objectives & Their Focus



[1 min for this slide]

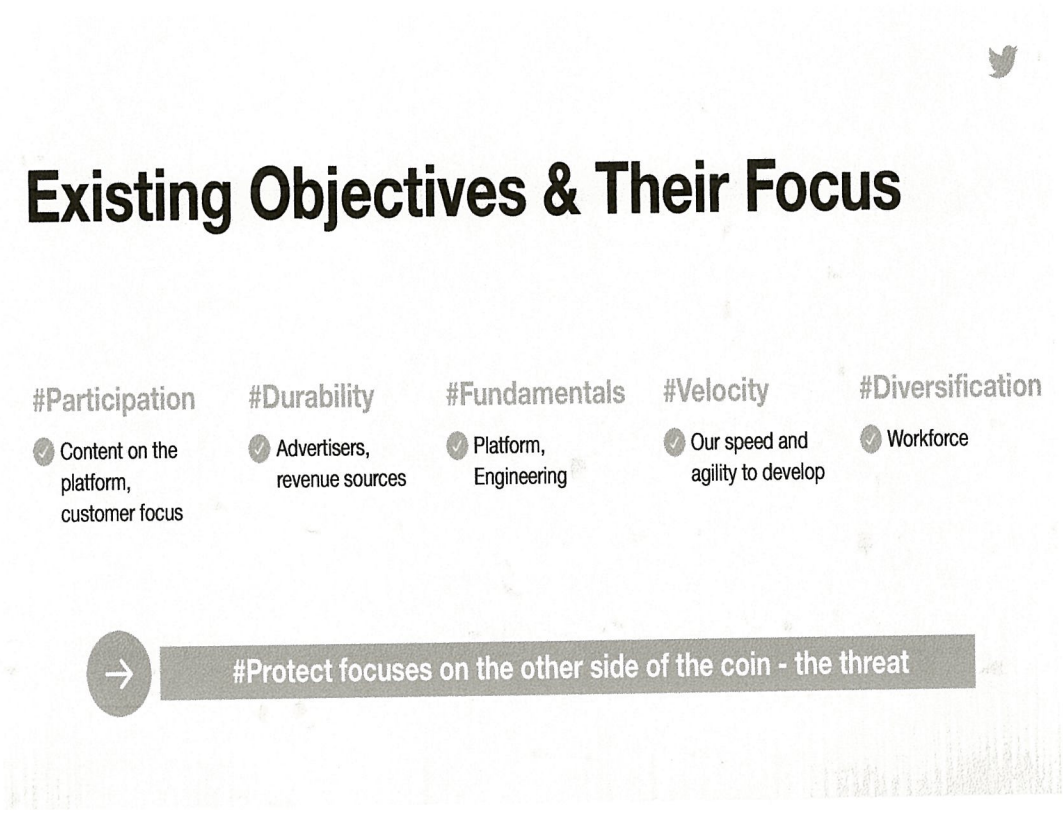
Looking across our Objectives we have significant focus on ourselves our people and workplace, our content, our platform and how we do engineering, our customers and their choices, and our partners and revenue sources.

I look at all of this as focusing on the spirit of #OneTeam

Unfortunately, not everyone is on #OneTeam and we need to focus on those people that aren't as well.

This is why #Protect is complementary.

Focus on the good things & people we want to help



[1 min for this slide]
Protect focuses on the baddies.. the threat. the other side of the coin.

How We'll Measure Success

Through 3 North Star Indicators

#PRO North Stars

Get the basics down and be excellent and efficient at them
None of our security or privacy & data-protection breaches happen due to our own poor hygiene or lack of due-diligence and follow-through.

Make our opponent's life more difficult, not ours
It is measurably and increasingly difficult (expensive) for bad actors to complete their objectives inside Twitter or on the Twitter platform. While doing so, we lead the industry in making the opaque fields of Security, Privacy, and Information Operations transparent and easier to understand.

When we expand the business we don't need to worry(*) about security and privacy
When we open new offices, data centers, products, and revenue lines we aren't overly worried about security, privacy, and human risk. Twitter's privacy, security, safety exposures grow more slowly than the expansion and growth of Twitter.

** We always need to think about them and be smart*

[3 min for this slide]
3 North stars and their indicators:

1 Basics - operational rigor, efficiency, and hygiene across privacy, security, safety. No more "ewww that was an embarrassing breach that we shouldn't have had". "Get rid of these large ***basic*** security and privacy gaps and exposures we have."

2 Make the baddies fire us because Twitter is a hard target, unrewarding, and risky for baddies to get involved with us - all the while ensuring our Customers hire us and it's easy and efficient for *us* get *our* jobs done. Make the safe and secure thing to do the easy and fast thing.

3 When we expand the business - launch new products, revenue streams, open offices in new countries, etc. We shouldn't be continuously re-exposing large areas of risk we don't need to. Our risk should grow minimally in comparison to the growth of our company. For example opening an office in a new country and putting engineers there shouldn't be as concerning as it is because of the exceptionally broad access all of our engineers have to critical systems and sensitive customer data services. (Our peers aren't carrying this repeated exposures the same way we are)

#PRO Key Results (KRs)

Get the #Protect basics down and be excellent at them!
None of our security or privacy & data-protection breaches happen due to our own poor hygiene or lack of due-diligence and follow-through.

End of 2022 KRs:

- The number of **internally identified vulnerabilities** goes up by at least **50%**, while the number of **externally identified vulnerabilities** goes down by at least **20%**.
- **100%** of newly launched products & features are in **compliance with our SDLC** and contain a valid threat model. More than **20%** of legacy products & features are in compliance with SDLC requirements.

[2 min for this slide]
Increasing the number of vulnerabilities we are internally finding proactively -> external discoveries start going down... meaning we are better at finding these issues before others find them and we are addressing them
AND
quickly get to 100% of our newly launched products and features launch in compliance with security/privacy and SDLC regulatory ...

...It's more critical, initially, that we not launch new vulnerabilities and incidents than it is to go back and find and address all of the problem areas in legacy products and features. Demonstrate to regulatory agencies that we have improved processes and procedures in place moving forward.

if we keep launching new security/privacy incidents after we have said we fixed our broken ways - we may encounter punishments will be refused to compete fairly w/ peers (data off limits), fines: penalties, reduced access to markets
parallel

#PRO KRs

Make our opponent's life more difficult, not ours!
It is measurably and increasingly difficult (expensive) for bad actors to complete their objectives inside Twitter or on the Twitter platform. While doing so, we lead the industry in making the opaque fields of Security, Privacy, and InfoOperations transparent and easier to understand.

End of 2022 KRs:

- We complete a **full inventory** of our manual and automated moderation and security detections and responses.
- Twitter has implemented **baseline language capabilities** to meet existing human-support SLAs for **100% of the top 20 languages**, and are also able to onboard new human support within 2 business days a major event.
- Twitter's **transparency efforts**, including a regularized, risk-managed cadence of Adversary Activity disclosures and a first-in-the-industry annual **"Threats to the Public Conversation" Report** by no later than Q3 2022, lead to an **observed change in the behavior of tracked bad actors** (whose activities we disclose/discuss in the report).

KR NS 2 complete inventory of ~~man~~ moderation & security actions ?
mini-max it (Fei-Fei)

[3 min for this slide]

Building a full inventory of all of our security detection and response activities -- whether formally captured playbooks or adhoc and institutional knowledge. We need to know not just the things we are and are not doing but also the things we have automated and do manually ~~(hint - a *lot* of manual solutions presently~~ -- while the bad actors are doing more and more ~~automated and at scale).~~ mini max

Protect needs to do it's work across all languages - because the people who don't have Twitter's best interests in mind work across langauges. Using a language other than one of the few we presently have good coverage across can't be a free pass for bad actors on the platform or in our threat safety work. English is not a free pass

It should become obvious how growing language capabilities will be valuable across the company.

The third measure in north star 2 starts by expanding the company's current work in transparency around Information Operations.

One way to drive up "cost" to bad actors is to shine a light on them and their activities. We start by measuring changes in their behavior due to experiments with the types of information and light we shine on them. - Game Theory

fighter

#PRO KRs

When we expand the business we don't need to worry* about security and privacy!
Twitter's privacy, security, safety exposures grow more slowly than the expansion and growth of Twitter.

End of 2022 KRs:

- **100% of production access** by Tweeps is logged and routinely audited to ensure **access is limited** to appropriate and validated business needs.
- Legacy persistent **privilege grants** are drawn down to **33%** of Q1 2022. (Basic)
- Independent auditor identifies **all promises we have made** to customers as it relates to how we handle their data and information, and we have determined where we are and are not in compliance with what we have promised.

Not afraid to have engineers anywhere: NSA, India, France

[2 min for this slide]

The measures start with understanding these repeated large concerns and exposures we keep fretting about over and over again with new offerings and expansions.

Drawing down some of the key legacy exposures and getting an independent auditor to identify all of the promises we have made to customers around how we protect them and their data. In this I am sure we will find other areas of repeated large exposures that we are reliving over and over with our new offerings and expansions.

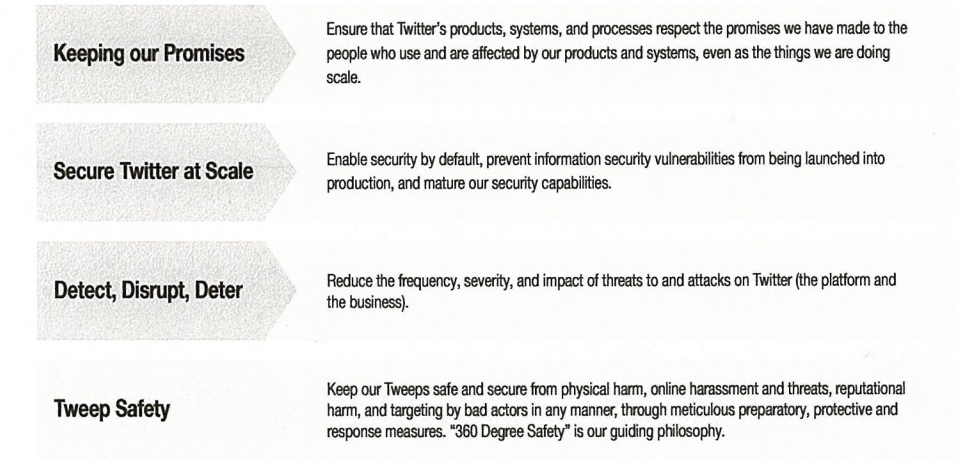
Tools and people for new products, privacy, fleets, spaces, are valuable, reusable tools, - not re-usable code-related exposures.

We've made many promises to customers and regulators about how we keep them safe and handle their data - we aren't sure we are keeping those promises - each new world we enter - cannot bring immediate broken promises.

13

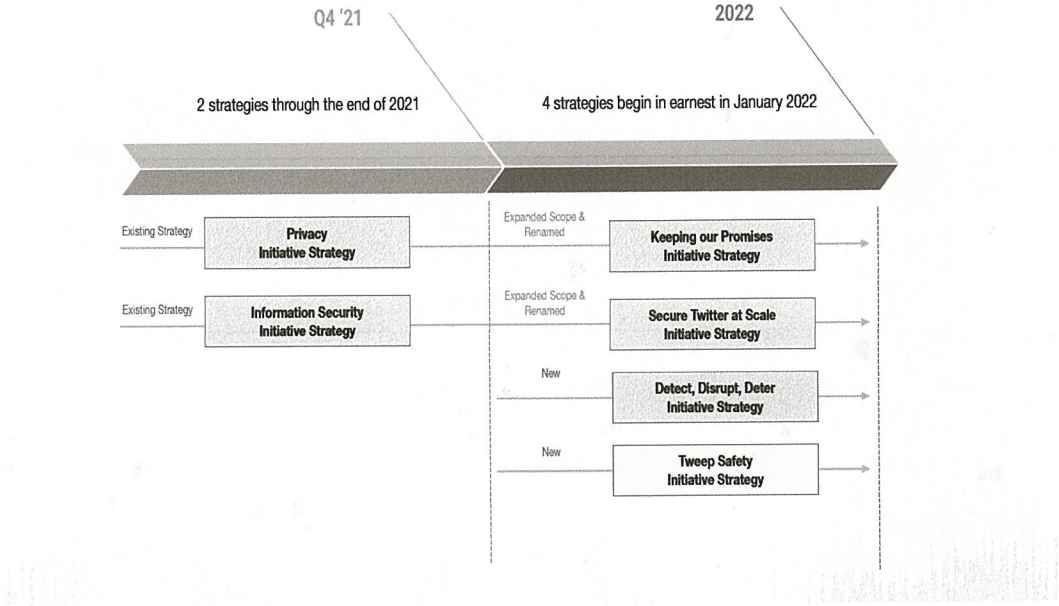
4 Initiative Strategies

#Protect Initiatives



[2 min for this slide]
There are 4 Initiatives within the #CON Obj that have been built or rebuilt to help us achieve this Objective.
We will go through each at a high-level. It is important to note up front, that these 4 Initiatives map to all 3 of the #CON North Stars. We intentionally set it up this way because of (1) the nature of the work (i.e., Security, privacy, threat detection/disruption, and safety work overlaps in fundamental ways, such that moving the needle against one north stars requires work that would also start to move the needle against other north stars.) and (2) to ensure the Obj is as cross-functional as it needs to be to be successful.
(if pressed: detailed mapping of Workstreams to north stars and KRs here)

#Protect will Launch in Phases

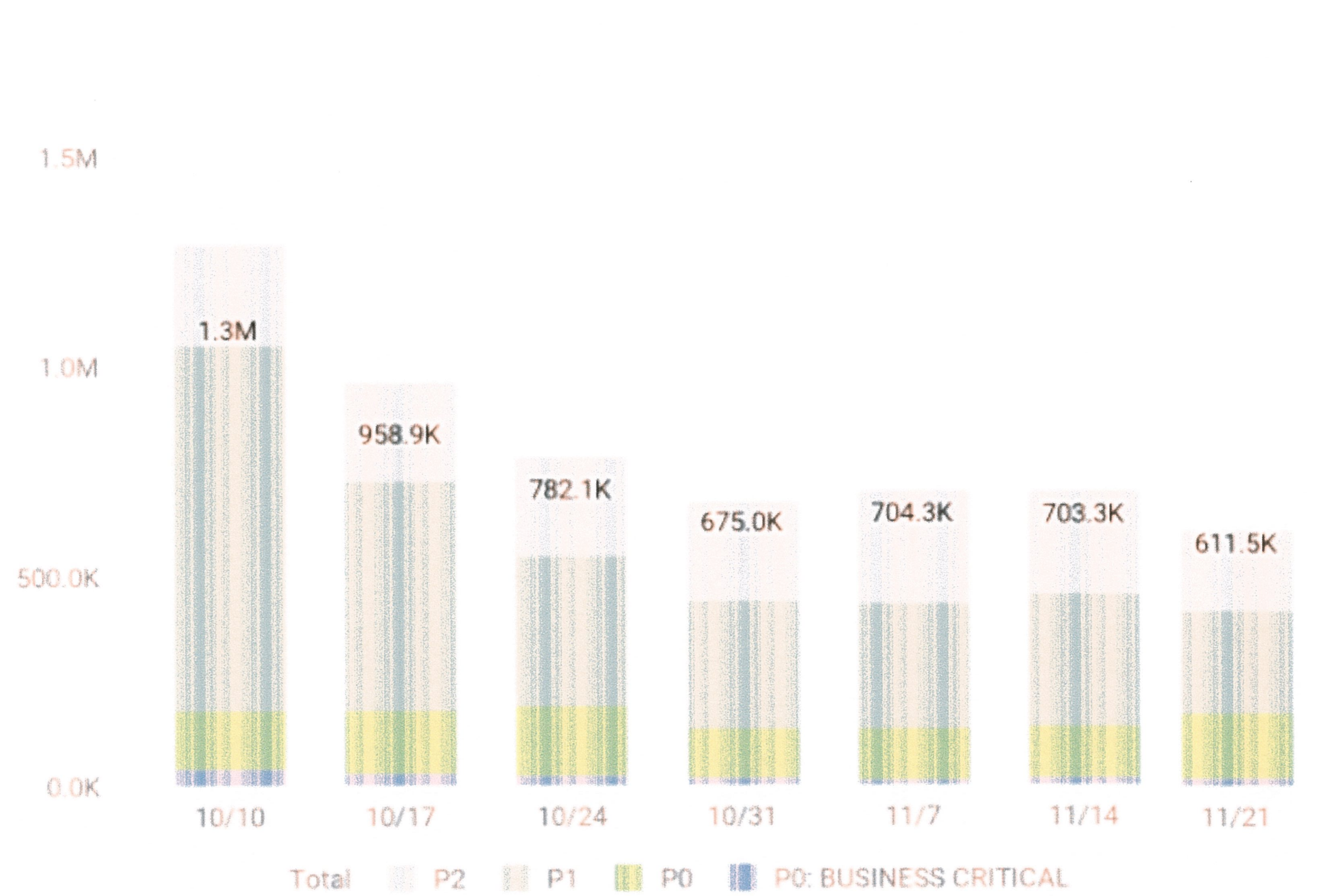


[1 min for this slide]

Suggested speaking notes:

- At the start of Q2, launched 2 Initiatives for H2 2021: Information Security and Privacy -- previously combined as one Initiative in #FUN, but now separated and rebooted.
- We used the rest of Q3 2021 to build, socialize, and align on the full Obj, including further refinement of the InfoSec and Privacy Initiatives
- Moving into 2022, we'll have 4 initiatives: With two new initiatives - Detect/Deter/Disrupt and Tweep Safety. We'll also expand the scope of the InfoSec and Privacy initiatives to fully support the #CON measures of success. We've renamed them as you can see here on the slide to be more indicative of their expanded scope.

Appendix


1.5M
1.0M
500.0K
0.0K
1.3M
958.9K
782.1K
675.0K
704.3K
703.3K
611.5K
10/10
10/17
10/24
10/31
11/7
11/14
11/21
Total
P2
P1
P0
P0: BUSINESS CRITICAL

Verification Volume Summary

Incoming, Reviewed and Backlog Volumes