Overview­

|  |  |
| --- | --- |
| Purpose | This guidance document outlines the roles, activities, and cross-functional coordination to support a MCS related cybersecurity bulletin publication, or to support an urgent cybersecurity action. |
| Scope | Cybersecurity bulletin or action involving a product manufactured or distributed by the Medtronic MCS Operating Unit (OU). |
| Roles | Action Plan Coordinator  Cybersecurity POC  Cross-functional team comprised of:   * Cybersecurity Engineer or representative * PSO (Product Security Office) Engineer or representative * Product Owner or representative * Marketing * Regulatory * Patient and Technical Services * Quality Engineer * Operating Unit and Functional VPs |

Table of Contents

[Terms and Definitions 2](#_Toc192820277)

[1. Security Bulletin Action Process Flow 3](#_Toc192820278)

[1.1 Security bulletin action 3](#_Toc192820279)

[1.2 Identify team and stakeholders 3](#_Toc192820280)

[1.3 Develop action plan 5](#_Toc192820281)

[1.4 Review/approve action plan with stakeholders 5](#_Toc192820282)

[1.5 Develop deliverables per plan 6](#_Toc192820283)

[1.6 Review/refine/approve deliverables 6](#_Toc192820284)

[1.7 Route and approve deliverables 7](#_Toc192820285)

[1.8 Publish/Distribute deliverables 7](#_Toc192820286)

[1.9 Monitor media attention 8](#_Toc192820287)

[2. Urgent Action Process Flow 8](#_Toc192820288)

[2.1 Urgent action is necessary by MDT MCS Cybersecurity 8](#_Toc192820289)

[2.2 Mobilize action team 9](#_Toc192820290)

[2.3 Plan necessary actions 10](#_Toc192820291)

[2.4 Review and approve communications 11](#_Toc192820292)

[2.5 Complete planned actions 11](#_Toc192820293)

[2.6 Monitor media attention 11](#_Toc192820294)

[Appendix A – Roles and Responsibilities 12](#_Toc192820295)

[Appendix B – Action Plan Template 12](#_Toc192820296)

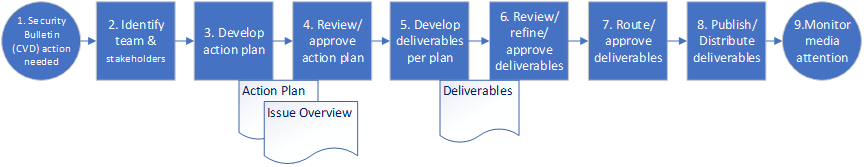
[Cybersecurity Action Plan 12](#_Toc192820297)

Terms and Definitions

|  |  |
| --- | --- |
| MCS | Mechanical Circulatory Support |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CVE | Coordinated Vulnerabilities and Exposures |
| ICS | Industrial Control Systems |
| MDT | Medtronic PLC |
| NIST | National Institute of Standards and Technology |
| NVD | National Vulnerability Database |
| PCS | Patient Care Services |
| OU | Operating Unit |
| POC | Point of Contact |
| PR | Public Relations |
| PSO | Product Security Office |
| GSO | Global Security Office |
| SME | Subject Matter Expert |
| VP | Vice President |
| HVAD | Heartware Ventricular Assist Device |

# Security Bulletin Action Process Flow

This flow diagram outlines the steps that support a security bulletin publication involving a product manufactured or distributed by the Medtronic MCS OU.



## Security bulletin action

MCS Cybersecurity Leadership in collaboration with Product Security Office (PSO) have determined that a security bulletin publication is necessary. MCS Cybersecurity will reach out to quality as a trigger to execute this action plan process. A team of subject matter experts and stakeholders is then identified to plan the necessary activities and deliverables.

## Identify team and stakeholders

The roles and activities related to identifying the action team and related stakeholders are as follows. See Appendix A for Roles and Responsibilities related to this process.

|  |  |
| --- | --- |
| Role | **Activity** |
| MCS Cybersecurity Leadership /Post-Market Quality | Identify a cross-functional action team based on the relevant MCS products that comprises SMEs from the following disciplines:   * Action Plan Coordinator * Cybersecurity POC (such as a Cybersecurity Director) * PSO (Product Security Office) Engineer or Representative * Product Owner or Representative * Marketing and Product Marketing * Communications * Regulatory * Patient and Technical Services * Quality |
| Action Team | Identify OU VPs, along with Functional VPs as reviewers and approvers of the Action Plan, and communication deliverables (including the Security Bulletin). These stakeholders are input into the review/approvals grid applicable to each deliverable. See *Example of a review/approval Grid.*   * MCS OU VP for relevant Product (e.g., HVAD) * MCS Field Services (including PTS) * MCS Communications * MCS Marketing and Product Marketing * MCS Regulatory * MCS Quality * MCS Legal |
| Action Plan Coordinator | The coordinator (such as a program manager) will establish meetings and manage the action plan throughout the effort.  Considerations:   * Establish a team’s channel to support team coordination and communications, and file sharing. * Establish a cadence of team meetings to facilitate plan maintenance, execution, and team updates. |
| Cybersecurity POC | The Cybersecurity POC is responsible for general cybersecurity leadership and executive updates. They are the point of contact for the OU and Function VPs.  Note: Early notification to internal leadership is recommended even in cases where the issue is not fully understood or characterized. |
| OU and Function VPs | OU VPs and Functional VPs will review and approve the deliverables such as the action plan, and any communication deliverables (including the security bulletin). These stakeholders are input into the review/approvals grid applicable to each deliverable. See *Example of a review/approval Grid.*   * MCS OU VP for relevant Product (e.g., HVAD) * MCS Field Services * MCS Communications * MCS Marketing * MCS Regulatory * MCS Quality * MCS Legal |

## Develop action plan

The roles and activities related to developing the action plan, and refining the plan based on any feedback are as follows.

|  |  |
| --- | --- |
| Role | **Activity** |
| Action Team | **Build the action plan:** As a cross-functional team, determine the action plan activities, completion dates, order of events (dependencies), ownership, etc.  See Appendix B – Action Plan Template for guidance on action plan content |
| Action Team/or Designee | **Build the Issue Overview:** Recommendation is to build a brief presentation to facilitate VP understanding of the issue and plan overview. |
| Activity Owners | Activity owners should define activities related to their function. Activities include (but are not limited to):   * Action Plan creation and approval (see Appendix B – Action Plan Template) * OU and functional Leadership presentation * Deliverable (security bulletin/communications) creation and approval * Media Q&A for reporters * Quality 806 applicability determinations, RPI creation and assessment * Marketing field notifications for awareness * PSO Security bulletin subscribers’ notifications   Consider planning activities related to: Patient and Tech Services reviews, Legal and/or Privacy reviews, MarComm, language translations, FDA feedback cycles, and significant feedback/review cycles from internal stakeholders. Note: There can be a significant investment in refining and addressing comments. |
| Action Plan Coordinator | Ensures the action plan is created and readily accessible by the team. |

## Review/approve action plan with stakeholders

The roles and activities related to reviewing the action plan, refining based on any feedback, and approving the plan, are as follows.

|  |  |
| --- | --- |
| Role | **Activity** |
| Cybersecurity POC | Cybersecurity POC should facilitate the internal reviews/approvals with OU and Functional VPs. Activities include (not limited to):   * Review Issue Overview with VPs as appropriate (this may be a small set of high-feedback VPs) * Review the action plan with VPs and request review feedback and subsequent approvals are documented in approval grid within the action plan * Action plan approval (See Appendix B – Action Plan Template for more details) |
| Action Team | Address any action plan feedback by reviewers.  Note: There can be a significant investment in refining and addressing comments. |
| OU and Function VPs | Gains understanding of the issue and reviews the action plan. When feedback is addressed, VPs will approve the plan by entering a date into the approval grid within the action plan. See *Example of a review/approval Grid.* |
| Action Plan Coordinator | Ensures the action plan status is maintained and team is updated with status as appropriate. |

## Develop deliverables per plan

The roles and activities related to developing and drafting the deliverables, and refining deliverables based on team collaboration and feedback are as follows.

|  |  |
| --- | --- |
| Role | **Activity** |
| PSO SME/Security POC | Develop the contents of the security bulletin in alignment with any in-flight customer/field communication content. PSO facilitates collaboration on security bulletin and determines if CVE / ICS CISA Disclosure is needed. |
| Product Owner/SME | Develop the contents of the plan deliverables in alignment with any in-flight security bulletin content. |
| Activity Owner | Ensure any activity that is owned at this stage is being executed. |
| Action Plan Coordinator | Ensures any deliverable, security bulletin, and communications are documented and readily accessible by the team. |

## Review/refine/approve deliverables

The roles and activities related to executing reviews, refining deliverables, and completing approvals are as follows.

|  |  |
| --- | --- |
| Role | **Activity** |
| Cybersecurity POC | Cybersecurity POC should facilitate the reviews/approvals for all deliverables *(i.e., one message to all approvers for all deliverables works well)*  Include the Review/Approval grid at the top of each deliverable.  Specify dates to receive comments and for final review comments *(to facilitate addressing comments)* |
| PSO SME | Gather FDA feedback on security bulletin draft content (when applicable). |
| Action Team | Address any deliverable feedback by reviewers. Coordination of subsequent reviews directly with reviewers can expedite the feedback cycles. |
| OU and Function VPs | VPs will review the deliverables and add review comments and questions. When feedback is addressed, VPs will approve each deliverable by entering a date into the Review/Approval grid within each deliverable. *Note: approval grids are to be deleted from all deliverables when all reviews are complete.*  Support completion of dates to receive comments and for final review comments *(to facilitate addressing comments).* |
| Action Plan Coordinator | Ensures the action plan status is maintained and the team is updated with status as appropriate. |

Example of a Review/Approval Grid.

|  |  |  |
| --- | --- | --- |
| Name | OU/Function | Approval Date |
| *E.g. Jim Vogl* | *PCS* | *11/17/2024* |
| *E.g. Julia Bucheger* | *MCS Service* | *11/20/2024* |
| *E.g. Kathleen Janasz* | *MCS Communications* | *11/21/2024* |
| *E.g. Holly Vitense* | *MCS Marketing* | *11/19/2024* |
| *E.g. Carrie Schleis* | *MCS Quality* | *11/22/2024* |
| *E.g. Rita Guzzetta* | *MCS Regulatory* | *11/17/2024* |
| *E.g. Christina Rich* | *MCS Legal* | *11/21/2024* |

## Route and approve deliverables

The roles and activities related to routing and approving deliverables are as follows.

|  |  |
| --- | --- |
| Role | **Activity** |
| Product Owner/SMEs | Facilitate the reviews/approvals of deliverables in source systems (i.e., MedReview, Agile MAP, MarComm systems)  *Note: Ensure approval grids are removed from final deliverables* |
| Deliverable Approvers | Conduct review and approval (when appropriate) in the source system. |
| Action Plan Coordinator | Ensures the action plan status is maintained, and the team is updated with status as appropriate. |

## Publish/Distribute deliverables

The roles and activities related to publishing and distributing deliverables are as follows.

|  |  |
| --- | --- |
| Role | **Activity** |
| Product Owner/SMEs | Facilitate the distribution of field and customer-related deliverables. *Note: Ensure approval grids are removed from final deliverables* |
| PSO/Cybersecurity POC | SMEs facilitate the publication of security bulletins and subsequent subscriber notifications as appropriate. *Note: Ensure approval grids are removed from final deliverables.* |
| Action Plan Coordinator | Ensures the action plan closure is maintained and the team is updated with status as appropriate. |

## Monitor media attention

The roles and activities related to monitoring the media attention are as follows.

|  |  |
| --- | --- |
| Role | **Activity** |
| Product Owner/SME | Monitor media coverage and handle any response necessary.  Notify action team/internal stakeholders as appropriate. |
| PSO SME/Cybersecurity POC | Monitors for any changes in the security landscape for the vulnerability to determine if any changes are needed. *(i.e., updates in security bulletin, risk management)*  Monitor for any changes in media activity for communication to internal stakeholders.  Notify action team/internal stakeholders as appropriate. |

# Urgent Action Process Flow

This flow diagram outlines the steps necessary when an urgent cybersecurity action is determined necessary by MCS Cybersecurity Leadership in collaboration with the Product Security Office (PSO) that involves a product manufactured or distributed by Medtronic MCS. 

## Urgent action is necessary by MDT MCS Cybersecurity

This process supports urgent cybersecurity issues that require immediate action or communication, or an MDT response.

The roles and activities related to defining and delivering urgent cybersecurity actions are outlined in the following sections. Examples of urgent cases are as follows.

Urgent Cybersecurity Situations

|  |  |
| --- | --- |
| Urgent Example | **Description** |
| Exploit code released without prior MDT response | Exploitable code has been released related to possible vulnerabilities in MCS products actively used in the field, prior to any MDT formal evaluation or response. |
| Active attack on MCS fielded product | An active attack is exploiting possible vulnerabilities in MCS products that are actively used in the field. |
| MCS Software product is defaced | MCS software product that is actively used in the field, has been defaced or is otherwise not in full control of MDT MCS. |

## Mobilize action team

The roles and activities related to mobilizing the action team are as follows.

|  |  |
| --- | --- |
| Role | **Activity** |
| Cybersecurity leadership | Identifies an action team based on the relevant MCS products, from the following functions. See Appendix A for Roles and Responsibilities related to this process.   |  |  | | --- | --- | | Function | Team Members | | Cybersecurity SMEs (MCS Cybersecurity, PSO, GSO) | *(e.g. John Kelcher)* | | Product SMEs/Product Owners | *Depends on product* | | Communications (MCS/CORP) | *(e.g. Emily Dornfeld)* | | Quality | *(e.g. Melinda Kolstad)* | | Privacy | *(e.g. Linda Whitlock)* | | Legal | *(e.g. Christina Rich)* | | Regulatory | *(e.g. Laura Danielson)* | | Marketing | *Depends on product* |   Identify an action plan coordinator. This person is intended to manage the action planning and work streams as needed.  Initiate a team kick-off of the issue and communicate the urgency and any required timelines.  Identify Executive Team that will be informed of the issue and any necessary actions. |
| Action Plan Coordinator | Initiate an action plan (See Appendix B – Action Plan Template for more details)  Create any team collaboration/status meetings  Create any needed Teams channels or other collaboration forums  Identify a conference room to serve as a team home-base |
| Executive Team | Executive team will be informed of necessary actions and will escalate messaging laterally and upward as necessary.   |  |  | | --- | --- | | Function | Executive Team Members | | Cybersecurity (MCS Cybersecurity, PSO, GSO) | *(e.g. Andy Hoff/Jennifer DeCarli)* | | Product Leadership | *(e.g. Jim Vogl)* | | Communications (MCS/CORP) | *(e.g. Kathleen Janasz)* | | Quality | *(e.g. Carrie Schleis)* | | Privacy | *(e.g. Lauren Ulvestad)* | | Legal | *(e.g. Christina Rich)* | | Regulatory | *(e.g. Rita Guzzetta)* | | Marketing | *(e.g. Craig Doerrmann)* | |

## Plan necessary actions

The roles and activities planning necessary actions are as follows. See Appendix B – Action Plan Template for guidance on action plan content.

|  |  |
| --- | --- |
| Role | **Activity** |
| Action Team | Identify Work streams/Deliverables –define the work streams as necessary, identify any communication(s) needed, as well as the audience and the activities needed for publication based on timelines/goals.  Identify Due Date –start by defining communication date requirements and define activities and timelines that meet that date.  Identify Risks/Roadblocks – identify vacations, holidays, procedural/compliance dependencies. Consider Geography roadblocks/translation needs.  Revise plan/team members to eliminate risks.  Document and Inform on the action plans – align with leadership on direction of action plans. Update leadership with execution progress and any milestones as they occur.  Ensure team members contribute to the schedule throughout as issue details develop. |
| Action Plan Coordinator | Maintain the action planning and work stream progress.  Facilitate team collaboration as appropriate.  Document discussions, decisions, milestones as appropriate. |
| Quality | Determine 806 applicability and any need for RPI creation. |
| Cybersecurity Leadership | Regularly communicate with executive team on action planning, issue developments, and overall progress. |

## Review and approve communications

The roles and activities related to reviewing and approving any communication is as follows.

|  |  |
| --- | --- |
| Role | **Activity** |
| Action Team | Preview communications with Action Team and leadership team.  Refine communications as real-time as possible.  Route/Approve communications as necessary.  Distribute/share final copies of communications as appropriate. |
| Quality | Complete Corrections and Removal (i.e., 806) review as appropriate. |
| Action Plan Coordinator | Maintain the action planning and work stream/deliverable progress |
| Cybersecurity Leadership | Regularly communicate with executive leadership on action planning, issue developments, and overall progress. |

## Complete planned actions

The roles and activities related to completing all planned actions are as follows.

|  |  |
| --- | --- |
| Role | **Activity** |
| Action Plan coordinator | Maintain the action planning and work stream progress.  Facilitate team collaboration as appropriate.  Document discussions, decisions/conclusions as appropriate. |
| Action Team | Execute to any work streams defined for the effort.  Coordinate any peer review for deliverables such as communication deliverables.  Participates regularly in any collaboration forum.  Share any final deliverables/milestones as appropriate. |
| Cybersecurity Leadership | Cybersecurity leadership will communicate any executive leadership updates, decisions, or any future strategic direction.  Complete any functional conclusions as needed |
| Product Owners/SMEs | Facilitate the distribution of field and customer related deliverables. Share any final deliverables/milestones as appropriate. |

## Monitor media attention

The roles and activities related to monitoring the media attention are as follows.

|  |  |
| --- | --- |
| Role | **Activity** |
| Product Owners/SMEs | Monitor media coverage and handle any response necessary.  Notify action team/internal stakeholders as appropriate. |
| PSO /Cybersecurity POC | Monitor for any changes in the security landscape for the vulnerability to determine if any changes are needed. *(i.e., updates in security bulletin, risk management considerations etc.)*  Monitor for any changes in media activity for communication to internal stakeholders.  Notify action team and internal stakeholders as appropriate. |

# Appendix A – Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Function** | **Role** | **Process Responsibility** |
| Cybersecurity MCS/PSO/GSO | MCS Product security point of contact | Cybersecurity POC coordinates overall internal messaging to leadership and overall cybersecurity and containment efforts.  PSO facilitates development and collaboration on SB and determines if CVE / ICS CISA Disclosure is needed. |
| Product Owner/Leadership | Product SME/Product Owner/MCS Info Systems & Services | Represents the voice of the product in all action planning activities and communication deliverables. Facilitates collaboration with product SMEs for communications content, audience definition and communication distribution (US/OUS). |
| Communications | MCS Communications SME | Initiate communications development and facilitates collaboration on all communications including media Q+A. |
| Quality | Post Market Quality | Represents quality and risk management processes. May also serve as the Action Plan coordinator.  Facilitates collaboration on any quality deliverables as needed. |
| Regulatory | Regulatory Engineer/Lead | Represents regulatory in action planning, FDA outreach and communications’ reviews. |
| Marketing | MCS Global Strategic Marketing SME | Represents marketing in action planning, and communications’ reviews. |

# Appendix B – Action Plan Template

## Cybersecurity Action Plan

**Purpose:**

The purpose of this action plan contains the plan scope, and deliverable activities that will be executed in support of a MCS related urgent communication. It is expected that the information contained in this document will be led by Cybersecurity leadership and Action Plan coordinator. VP review and approvals of the plan are contained within this plan – See VP Plan Approval Grid.

**Scope:**

Describe products impacted or related to the vulnerability.

**Issue Description:**

Description of the issue, security triggers, system architecture that gives a general overview.

**Short-term/Long-term Objectives:**

List general objectives of this action plan.

**Investigation and Conclusions:**

Describe any investigations/analysis of the issue, system architecture etc. List any documentation such as RPIs/SIIA or other initial conclusions or key findings.

|  |  |  |
| --- | --- | --- |
| Record Type | ID | Title |
| *E.g. RPI* | *321123* |  |
| *E.g. SIIA* | *D000123123* |  |

**Helpful References:**

List any references to CVEs or other information that gives context to the issue, system arch, investigation etc.

**VP Plan Approval Grid:**

List OU and Function VP stakeholders that need to review and approve this action plan.

|  |  |  |
| --- | --- | --- |
| Name | Organization | Plan Approved on: |
| *E.g. Jim Vogl* | PCS |  |
| *E.g. Julia Bucheger* | MCS Services |  |
| *E.g. Kathleen Janasz* | MCS Communications |  |
| *E.g. Holly Vitense* | MCS Marketing |  |
| *E.g. Carrie Schleis* | MCS Quality |  |
| *E.g. Rita Guzzetta* | MCS Regulatory |  |
| *E.g. Christina Rich* | MCS Legal |  |

**List of Action Plan Deliverables:**

The activities, owners, and approvers necessary to deliver a coordinated set of deliverables along with the needed security bulletin. See below for an example deliverable List.

|  |  |  |
| --- | --- | --- |
| Deliverable | Audience | Geographies |
|  |  |  |

**Action Plan Activities**

The activities, owners, and approvers necessary to deliver a coordinated set of deliverables along with the security bulletin.

Note: Ensure activities such as addressing OU VP review comments and FDA security bulletin reviews are planned with enough time in the schedule.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Target Completion Date | Activity | Status | Owner | Approvers | Notes |
|  |  |  |  |  |  |

|  |
| --- |
| **Example Deliverable List** |

|  |  |  |
| --- | --- | --- |
| Deliverable | Audience | Geographies |
| *Field Communication* | *US and Geo Partners* | *US/OUS Geo partners* |
| *Customer (direct) communication* | *Mainspring users with Mirth* | *US* |
| *Security Bulletin* | *Global* | *Global* |

**Example Action Plan**

Example considering Mirth Connect Vulnerability 2023

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MIRTH Security Vulnerability Action Plan - Nov 2023 | |  |  |  |
| **Completion Date (estimate)** | **Activity** | **Status** | **Responsible** | **Contributors/Approvers** |
| **WEEK OF Oct 30th** | Build action plan and complete technical eval of MCS impacts |  |  |  |
| **30-Oct** | Draft all actions in action plan  Update and socialize action with the team | Done | Melinda/Team | John K, Emily, Matt, Thomas, Seema, Katie |
| **30-Oct** | Conduct system installation testing | Done | John K | MCS Product Security, Mainspring SMEs |
| **31-Oct** | Draft Issue Overview (this is for VP understanding) | Done | Emily D/John K | John K, Emily, SMEs |
| **1-Nov** | Create RPI if determined needed | Done | Melinda |  |
| **1-Nov** | Socialize action plan with VPs (ensure comments and review dates are clear) | Done | John K | OU and Function VPs |
| **2-Nov** | Align MDT PCS additional leadership - Julia B, Angel R. |  | John K | Seema addition in team meeting, (cc Diva JZ, Prakash) |
| **3-Nov** | Address action plan comments (team review) | Done | Team | John K, Emily, Matt, Thomas, Seema, Katie etc |
| **3-Nov** | Start draft of Security Bulletin | Done | Matt V/John K | PSO, Mainspring SMEs |
| **WEEK OF Nov 6th** | Draft and finalize: Action Plan, Security Bulletin, MCS Field notice, Customer communication |  |  |  |
| **6-Nov-9-Nov** | Socialize final Action plan and gather VP approval dates | Done | John K | OU and Function VPs |
| **6-8, Nov** | **Continue draft of** Security Bulletin | Done | Matt V/John K | PSO, Mainspring SMEs |
| **6-8, Nov** | **Draft** Customer comm, MCS field notice | Done | Katie M, Seema G | TS, Reg, Quality, Marketing, Mainspring TS |
| **8, Nov** | Add approver/Stakeholder grid to the top of the Customer Letter, Field Communication, Security Bulletin | Done | Emily, Thomas | Jim V, Julia B, Kathleen J, Holly V, Chris Reed (SB), Jim P, Carrie S. Laura D, Christina R |
| **8-Nov** | Confirm steps with Patient and Tech Services (to understand how an HCP would determine that they are using Mainspring) | Done | Thomas | Christopher Z |
| **8-Nov** | **Draft** 806 rationale for RPI | Done | Melinda | Quality |
| **9,10-Nov** | Team to **review** bulletin | Done | Matt V/John K | PSO, MCS Prod Security, Mainspring SMEs/TS |
| **9,10-Nov** | Team to **review** Customer Comm, MCS field Notice | Done | Katie M, Seema G | SME team, OU and Function VPs |
| **10-Nov** | **Inform** RSM leadership in meeting as awareness of action plans and progress | Done | Katie M, Seema G |  |
| **WEEK OF Nov 13th** | Gather leadership comments and finalize with SMEs and VPs |  |  |  |
| **13,14-Nov** | Gather OU/VP SMEs feedback on Security Bulletin |  | Matt V/John K | PSO, MCS Prod Security, Mainspring SMEs/TS |
| **13,14-Nov** | Gather OU/VP SMEs feedback on Communication, field notice | Done | Katie M, Seema G | TS, Reg, Quality, Marketing, Mainspring TS |
| **15,16-Nov** | Address all feedback (in team meeting recommended) | Done | Katie M, Seema G | TS, Reg, Quality, Marketing, Mainspring TS |
| **15-Nov** | **Review/Finalize** 806 rationale | Done | Melinda | Quality leadership |
| **17-Nov** | Align the Security Bulletin with comms updates | Done | Matt V/Thomas |  |
| **17-Nov** | Send comm/SB updates to high-feedback VPs who are SMEs (requesting review by EOD Nov 20th) - *Confirmed that VP completed review in the AM* | Done | John K | Jim V, Julia B, Kathleen J, Holly V, Chris R (SB), Jim P, Carrie S. Laura D, Christina R (Julia B may want a heads up prior to this email) |
| **WEEK OF Nov 20th** | Address all comments and align plan/finals with SME VPs |  |  | *Week contains thanksgiving* |
| **20-Nov** | Meeting to Touch base with Julia and William | Done | Katie M, Seema G | Julia B, William H |
| **20-22-Nov** | Are there more updates/comments? Finalize any in a team meeting and send again final version | Done | Team Meeting/John K | Ensure all VPs see all final changes. |
| **22-Nov** | John K to send to Jim V finals. Jim V to provide to Kweli's staff | Done | John K/Jim V | Jim V, Julia B, Kathleen J, Holly V, Chris Reed (SB), Jim P, Carrie S. Laura D, Christina R |
| **WEEK OF Nov 27th** | Stage SB and route/approve, Customer communication. Updates to leadership as needed |  |  |  |
| **27-Nov** | Jim V to give MCS Leadership update atOU President staff meeting | Done | Jim V/John K | OU President staff |
| **27-Nov** | **Route/approve** customer communication and MCS field notices in MedReview | Done | Katie M, Seema G | Marketing (Katie, Seema, Craig D), Regulatory (Laura) |
| **28-Nov** | Stage Security Bulletin | Done | Matt V/Thomas | PSO, and notify team |
| **29-Nov** | Milestone: Send MCS field Notice/Tech Support notice *(reference general link)* | Done | Katie M, Seema G | MCS Field Leadership (RSMs, RVPs, DM, & DSMs)/PTS leadership |
| **29-Nov** | Milestone: Send Geo partner notice (send comm materials for distribution - OUS scope) *(reference general link)* | Done | Katie M, Seema G | PCS regional contacts |
| **30-Nov** | Milestone: Publish security bulletin (Thursdays) - ~7 am CST | Done | Matt V | Thomas |
| **30-Nov** | Milestone: Send customer communication *(US ~37, OUS out of scope). This references a general link to the location of the security bulletin.* | Done | Katie M, Seema G | Katie M, Seema G (RS email) |
| **1-Dec** | Status update on Vulnerability (via the channel) | Done | Matt V/PSO |  |
| **1-Dec** | Email to subscribed email addresses will be sent out on December 1 around 9:00 AM Central Time. | Done | Corp. External Comm |  |
| **1-Dec** | Email from PSO to H-ISAC vulnerability contacts informing them of the new disclosure will be sent out on December 1 around 12:00 PM Central Time. |  | PSO |  |